university of groningen

University Medical Center Groningen

University of Groningen

Explicit Chabauty--Kim for the Split Cartan Modular Curve of Level 13

Balakrishnan, Jennifer; Dogra, Netan; Müller, Jan Steffen; Tuitman, Jan; Vonk, Jan

Published in:
Annals of mathematics

DOI:
10.4007/annals.2019.189.3.6

IMPORTANT NOTE: You are advised to consult the publisher's version (publisher's PDF) if you wish to cite from it. Please check the document version below.

Document Version
Final author's version (accepted by publisher, after peer review)

Publication date:
2019

Link to publication in University of Groningen/UMCG research database

Citation for published version (APA):
Balakrishnan, J., Dogra, N., Müller, J. S., Tuitman, J., & Vonk, J. (2019). Explicit Chabauty--Kim for the Split Cartan Modular Curve of Level 13. *Annals of mathematics*, *189*(3), 885-944. https://doi.org/10.4007/annals.2019.189.3.6

Copyright
Other than for strictly personal use, it is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license (like Creative Commons).

The publication may also be distributed here under the terms of Article 25fa of the Dutch Copyright Act, indicated by the “Taverne” license. More information can be found on the University of Groningen website: https://www.rug.nl/library/open-access/self-archiving-pure/taverne-amendment.

Take-down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Downloaded from the University of Groningen/UMCG research database (Pure): http://www.rug.nl/research/portal. For technical reasons the number of authors shown on this cover page is limited to 10 maximum.

Download date: 05-05-2023

EXPLICIT CHABAUTY–KIM FOR THE SPLIT CARTAN MODULAR CURVE OF LEVEL 13

JENNIFER S. BALAKRISHNAN, NETAN DOGRA, J. STEFFEN MÜLLER, JAN TUITMAN, AND JAN VONK

Abstract. We extend the explicit quadratic Chabauty methods developed in previous work by the first two authors to the case of non-hyperelliptic curves. This results in an algorithm to compute the rational points on a curve of genus $g \geq 2$ over the rationals whose Jacobian has Mordell-Weil rank g and Picard number greater than one, and which satisfies some additional conditions. This algorithm is then applied to the modular curve $X_{\mathrm{s}}(13)$, completing the classification of non-CM elliptic curves over $\mathbf{Q}$ with split Cartan level structure due to Bilu–Parent and Bilu–Parent–Rebolledo.

Contents

1. Introduction

In this paper, we explicitly determine the rational points on $X_{\mathrm{s}}(13)$, a genus 3 modular curve defined over $\mathbf{Q}$ with simple Jacobian having Mordell-Weil rank 3. This computation makes explicit various aspects of Minhyong Kim's nonabelian Chabauty programme and completes the "split Cartan" case of Serre's uniformity question on residual Galois representations of elliptic curves. Moreover, the broader techniques are potentially of interest for determining rational points on other curves. The main technical development is an algorithm for computing Frobenius structures on the unipotent isocrystals which arise in the Chabauty–Kim method. We begin with an overview of Serre's question, outline our strategy to compute $X_{\mathrm{s}}(13)(\mathbf{Q})$ in the context of Kim's nonabelian Chabauty, and end with some remarks on the scope of the method in the toolbox for explicitly determining rational points on curves.

1.1. Modular curves associated to residual representations of elliptic curves.

If $E/\mathbf{Q}$ is an elliptic curve and ℓ is a prime number, then there is a natural residual Galois representation

$$\rho_{E,\ell} : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}(E[\ell]) \simeq \mathrm{GL}_2(\mathbf{F}_\ell).$$

Serre [Ser72] showed that if E does not have complex multiplication (CM), then $\rho_{E,\ell}$ is surjective for all primes $\ell \gg 0$.

Question (Serre)**.** *Is there a constant ℓ_0 such that $\rho_{E,\ell}$ is surjective for all elliptic curves $E/\mathbf{Q}$ without CM and all primes $\ell > \ell_0$?*

It is known that if ℓ_0 exists, then it must be at least 37. To tackle this question, one may use the fact that a maximal subgroup of $\mathrm{GL}_2(\mathbf{F}_\ell)$ is either a Borel subgroup, normalizer of (split or non-split) Cartan subgroup, or exceptional subgroup. The Borel and the exceptional cases were handled by Mazur [Maz78] and Serre [Ser72], respectively, and the case of normalizers of split Cartan subgroups (for $\ell > 13$) follows from Bilu-Parent [BP11] and Bilu-Parent-Rebolledo [BPR13], which we now recall.

For a prime ℓ, we write $X_{\mathrm{s}}(\ell)$ for the modular curve $X(\ell)/C_{\mathrm{s}}(\ell)^+$, where $C_{\mathrm{s}}(\ell)^+$ is the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbf{F}_\ell)$. Since all such subgroups $C_{\mathrm{s}}(\ell)^+$ are conjugate, $X_{\mathrm{s}}(\ell)$ is well-defined up to $\mathbf{Q}$-isomorphism. Bilu–Parent [BP11] proved the existence of a constant ℓ_{s} such that $X_{\mathrm{s}}(\ell)(\mathbf{Q})$ only consists of cusps and CM points for all primes $\ell > \ell_{\mathrm{s}}$. This was later improved by Bilu–Parent–Rebolledo [BPR13] who showed that the statement holds for all $\ell > 7$, $\ell \neq 13$. This proves that, for all primes $\ell > 7$, $\ell \neq 13$, there exists no elliptic curve $E/\mathbf{Q}$ without CM whose mod-ℓ Galois representation has image contained in the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbf{F}_\ell)$. However, they were unable to prove this statement for $\ell = 13$.

Bilu, Parent, and Rebolledo use a clever combination of several techniques for finding $X_{\mathrm{s}}(\ell)(\mathbf{Q})$, but one of the crucial ingredients is Mazur's method [Maz78] for showing an integrality result for non-cuspidal rational points on $X_{\mathrm{s}}(\ell)$. This relies on the statement

$$\mathrm{Jac}(X_{\mathrm{s}}(\ell)) \sim \mathrm{Jac}(X_0^+(\ell^2)) \sim J_0(\ell) \times \mathrm{Jac}(X_{\mathrm{ns}}(\ell))$$

proved by Chen [Che98], where $X_{\mathrm{ns}}(\ell)$ is the modular curve associated to the normalizer of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbf{F}_\ell)$, similar to the split case. Mazur's method applies whenever $J_0(\ell) \neq 0$, which is the case for $\ell = 11$ and $\ell \geq 17$. But since $J_0(13) = 0$, it follows that $\mathrm{Jac}(X_{\mathrm{s}}(13)) \sim \mathrm{Jac}(X_{\mathrm{ns}}(13))$ and $\mathrm{Jac}(X_{\mathrm{s}}(13))$ is absolutely simple, which is the underlying reason that their analysis does not succeed in tackling that case; they call 13 the *cursed level* in [BPR13, Remark 5.11].

In fact, Baran [Bar14a, Bar14b] showed that more is true: There is a $\mathbf{Q}$-isomorphism between $\mathrm{Jac}(X_{\mathrm{s}}(13))$ and $\mathrm{Jac}(X_{\mathrm{ns}}(13))$, and we further have

$$X_{\mathrm{ns}}(13) \simeq_{\mathbf{Q}} X_{\mathrm{s}}(13). \tag{1}$$

She derives (1) in two different ways: by computing explicit smooth plane quartic equations for both curves and observing that they are isomorphic [Bar14a] on the one hand, and by invoking Torelli's theorem [Bar14b] and an isomorphism between the Jacobians on the other. There is no known modular interpretation of the isomorphism (1). Since the problem of computing rational points on modular curves associated to normalizers of non-split Cartan subgroups is believed to be hard in general, this may give some indication why $X_{\mathrm{s}}(13)$ is more difficult to handle than $X_{\mathrm{s}}(\ell)$ for other $\ell \geq 11$.

Galbraith [Gal02] and Baran [Bar14a] computed all rational points up to a large height bound; they found 6 CM points and one cusp. In addition to Mazur's method, other standard approaches for proving that this is the complete set of rational points do not seem to work for $X_{\mathrm{s}}(13)$. The method of Chabauty and Coleman (see §1.3) fails as the rank of $\mathrm{Jac}(X_{\mathrm{s}}(13))$ is at least 3, and the genus of $X_{\mathrm{s}}(13)$ is 3. The Mordell–Weil sieve cannot be applied on its own, as $X_{\mathrm{s}}(13)(\mathbf{Q}) \neq \emptyset$. Descent and elliptic curve Chabauty also do not seem to work, as no suitable covers of $X_{\mathrm{s}}(13)$ are readily available.

In this paper we show, using quadratic Chabauty, that the only rational points on $X_{\mathrm{s}}(13)$ are indeed the points found by Galbraith and Baran.

Theorem 1.1. *The rational points on $X_{\mathrm{s}}(13)$ consist of six CM points and one cusp.*

Together with the results of Bilu–Parent and Bilu–Parent–Rebolledo, this allows us to complete the characterisation of all primes ℓ such that the mod ℓ Galois representation of a non-CM elliptic curve over $\mathbf{Q}$ is contained in the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbf{F}_\ell)$.

Theorem 1.2. *Let ℓ be a prime. Then there exists an elliptic curve $E/\mathbf{Q}$ without CM such that the image of $\rho_{E,\ell}$ is contained in the normalizer of a split Cartan subgroup if and only if $\ell \leq 7$.*

Via the isomorphism (1), we also find

Corollary 1.3. *We have $|X_{\mathrm{ns}}(13)(\mathbf{Q})| = 7$, and all points are CM.*

Remark 1.4. As was noted by Serre [Ser97] a complete determination of $X_{\mathrm{ns}}(N)(\mathbf{Q})$ for some N leads to a proof of the class number one problem. Corollary 1.3 therefore gives a new proof of this theorem.

1.2. **Notation.** Throughout this paper, $X/\mathbf{Q}$ denotes a smooth projective geometrically connected curve of genus $g \geq 2$ such that $X(\mathbf{Q}) \neq \emptyset$, with Jacobian J; we write $r := \mathrm{rk}(\mathrm{J}/\mathbf{Q})$ and $\rho := \mathrm{rk}(\mathrm{NS}(\mathrm{J}))$. Fix an algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$ and write $G_{\mathbf{Q}} := \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ and $\overline{X} := X \times \overline{\mathbf{Q}}$. Fix a base point $b \in X(\mathbf{Q})$ and a prime p of good reduction for X. The field $\mathrm{End}(J) \otimes \mathbf{Q}$ is denoted by K and we set

$$\mathcal{E} := \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^* \otimes \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^*.$$

Let T_0 the set of primes of bad reduction of X, and $T = T_0 \cup \{p\}$. We denote G_T for the maximal quotient of $\mathbf{Q}$ unramified outside T, and G_v for the absolute Galois group of $\mathbf{Q}_v$ for any prime v.

1.3. **Chabauty–Coleman and Chabauty–Kim.** Chabauty [Cha41] proved the Mordell conjecture for curves X as above, satisfying an additional assumption on the rank of the Jacobian. More precisely, Chabauty showed that the set $X(\mathbf{Q})$ is finite if $r < g$. Following Coleman [Col85], one may explain the proof as follows. The choice of base point b gives an inclusion of X into J, defined over $\mathbf{Q}$. On $\mathrm{J}(\mathbf{Q}_p)$ there is a linear integration pairing on the Jacobian defined by explicit power series integration on individual residue polydisks, extended via the group law

$$\mathrm{J}(\mathbf{Q}_p) \times \mathrm{H}^0(\mathrm{J}_{\mathbf{Q}_p}, \Omega^1) \longrightarrow \mathbf{Q}_p : (D, \omega) \mapsto \int_0^D \omega,$$

inducing a homomorphism

$$\log : \mathrm{J}(\mathbf{Q}_p) \longrightarrow \mathrm{H}^0(\mathrm{J}_{\mathbf{Q}_p}, \Omega^1)^*.$$

Via the canonical identification of $\mathrm{H}^0(\mathrm{J}_{\mathbf{Q}_p}, \Omega^1)$ with $\mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)$, this gives rise to the following commutative diagram:

(2)
$$\begin{array}{ccccc} X(\mathbf{Q}) & \longrightarrow & X(\mathbf{Q}_p) & & \\ \downarrow & & \downarrow & \searrow^{\mathrm{AJ_b}} & \\ \mathrm{J}(\mathbf{Q}) & \longrightarrow & \mathrm{J}(\mathbf{Q}_p) & \xrightarrow{\log} & \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^* \end{array}$$

where the Abel–Jacobi morphism $\mathrm{AJ_b}$ is defined to be the map sending a point x to the linear functional $\omega \mapsto \int_0^{[x-b]} \omega$. Chabauty's proof involves a combination of global "arithmetic" or "motivic" information with local "analytic" information. The global arithmetic input is that, when $r < g$, the closure $\overline{\mathrm{J}(\mathbf{Q})}$ of $\mathrm{J}(\mathbf{Q})$ with respect to the p-adic topology is of codimension ≥ 1. Hence there is a non-zero ω_{J} which vanishes on $\overline{\mathrm{J}(\mathbf{Q})}$, so that $X(\mathbf{Q})$ is annihilated by the function

(3)
$$x \longmapsto \mathrm{AJ_b}(x)(\omega_{\mathrm{J}}).$$

The local analytic input is that, on each residue disk of $X(\mathbf{Q}_p)$, $\mathrm{AJ_b}$ has Zariski dense image and is given by convergent p-adic power series, so the function in (3) can have only finitely many zeroes on each residue disk of $X(\mathbf{Q}_p)$. The non-trivial steps in solving for the function in (3) are:

- Determine, on each residue disk, the power series $\mathrm{AJ_b}$ to sufficient p-adic accuracy.
- Evaluate $\mathrm{AJ_b}(P_i)$ on a basis $\{P_i\}$ of $\mathrm{J}(\mathbf{Q}) \otimes \mathbf{Q}$.

With the aim of removing the restrictive condition $r < g$, Kim [Kim05, Kim09] has initiated a programme to generalise Chabauty's approach. As in the method of Chabauty and Coleman, one hopes to be able to translate Kim's approach into a practical explicit method for computing (a finite set of p-adic points containing) $X(\mathbf{Q})$ in practice for a given curve $X/\mathbf{Q}$ having $r \geq g$. However, in part due to the technical nature of the objects involved, this is a rather delicate task. Kim's results [Kim05] on integral points on $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ have been made explicit by Dan-Cohen and Wewers [DCW15] and used to develop an algorithm to solve the S-unit equation [DCW16, DC17] using iterated p-adic integrals. The work [BDCKW] of the first author with Dan-Cohen, Kim and Wewers contains explicit results for integral points on elliptic curves of ranks 0 and 1.

1.4. **Quadratic Chabauty.** One approach that has led to some explicit results involves p-adic heights. We now formalize this approach in elementary terms. Suppose $r = g$, and the p-adic closure of $\mathrm{J}(\mathbf{Q})$ has finite index in $\mathrm{J}(\mathbf{Q}_p)$. Then AJ_b induces an isomorphism $\mathrm{J}(\mathbf{Q}) \otimes \mathbf{Q}_p \simeq \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^*$, meaning that we cannot detect global points among local points using linear relations in AJ_b. The idea of the quadratic Chabauty method is to replace linear relations by bilinear relations. Suppose we can find a function $\theta : X(\mathbf{Q}_p) \to \mathbf{Q}_p$ and a finite set $\Upsilon \subset \mathbf{Q}_p$ with the following properties:

(a) On each residue disk of $X(\mathbf{Q}_p)$, the map

$$(\mathrm{AJ}_\mathrm{b}, \theta) \ : \ X(\mathbf{Q}_p) \longrightarrow \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^* \times \mathbf{Q}_p$$

has Zariski dense image and is given by a convergent power series.

(b) There exist
- an endomorphism E of $\mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^*$, and a functional $c \in \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^*$,
- a bilinear form $B : \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^* \otimes \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^* \to \mathbf{Q}_p$,

such that, for all $x \in X(\mathbf{Q})$,

$$\theta(x) - B(\mathrm{AJ}_\mathrm{b}(x), E(\mathrm{AJ}_\mathrm{b}(x)) + c) \in \Upsilon. \tag{4}$$

This gives a finite set of p-adic points containing $X(\mathbf{Q})$, since property (a) implies that only finitely many p-adic points can satisfy equation (4), and property (b) implies all rational points satisfy it. As in the Chabauty-Coleman method, finiteness is obtained by a combination of local analytic information and global arithmetic information. We shall refer to (θ, Υ) as a *quadratic Chabauty pair*. The objects E, c, and B will be referred to as its endomorphism, constant and pairing, respectively.

The goal of the quadratic Chabauty method is to be able to use a quadratic Chabauty pair (or several of them) to *determine* $X(\mathbf{Q})$. Let us clarify how the pair (θ, Υ) (as well as knowledge of the implicit E and c)[1] gives a method for determining a finite set containing $X(\mathbf{Q})$. For $\alpha \in \Upsilon$, define

$$X(\mathbf{Q}_p)_\alpha := \{x \in X(\mathbf{Q}_p) : \theta(x) - B(\mathrm{AJ}_\mathrm{b}(x), E(\mathrm{AJ}_\mathrm{b}(x)) + c) = \alpha\}.$$

By definition, $X(\mathbf{Q}) \subset \coprod_{\alpha \in \Upsilon} X(\mathbf{Q}_p)_\alpha$, and we focus on the problem of describing $X(\mathbf{Q}_p)_\alpha$. The following result gives an explicit equation for a finite subset of $X(\mathbf{Q}_p)$ containing $X(\mathbf{Q}_p)_\alpha$. Suppose we have $P_1, \ldots, P_m \in X(\mathbf{Q})$ such that

$$\mathrm{AJ}_\mathrm{b}(P_i) \otimes (E(\mathrm{AJ}_\mathrm{b}(P_i)) + c)$$

form a basis of $\mathcal{E}$ (see the end of §1.7 for a discussion of this assumption), and suppose that $\psi_1, \ldots, \psi_m$ form a basis of $\mathcal{E}^*$. Assume furthermore that we have $P_i \in X(\mathbf{Q}_p)_{\alpha_i}$, where $\alpha_i \in \Upsilon$. For $x \in X(\mathbf{Q}_p)$,

[1] In practice, one calculates E and c, but B is something one has to solve for, in the same way that one solves for the annihilating differential in the Chabauty-Coleman method.

define the matrix $T(x) = T_{(\theta,\Upsilon)}(x)$ by

$$T(x) = \begin{pmatrix} \theta(x) - \alpha & \Psi_1(x) & \dots & \Psi_m(x) \\ \theta(P_1) - \alpha_1 & \Psi_1(P_1) & \dots & \Psi_m(P_1) \\ \vdots & \vdots & \ddots & \vdots \\ \theta(P_m) - \alpha_m & \Psi_1(P_m) & \dots & \Psi_m(P_m) \end{pmatrix},$$

where $\Psi_i(x) := \psi_i(\mathrm{AJ_b}(x) \otimes (E(\mathrm{AJ_b}(x)) + c))$. Since B is a linear combination of the ψ_i, we get:

Lemma 1.5. *If $x \in X(\mathbf{Q}_p)_\alpha$, then we have* $\det(T(x)) = 0$.

1.5. **Quadratic Chabauty pairs for rational points.** The definition of quadratic Chabauty pairs is inspired by an approach for computing *integral* points on rank 1 elliptic curves [BB15], and more generally, on odd degree hyperelliptic curves [BBM16], which satisfy the assumptions of §1.4, as follows. Let $h : \mathrm{J}(\mathbf{Q}) \to \mathbf{Q}_p$ be the p-adic height function, then for $x \in X(\mathbf{Q})$ there is a decomposition [CG89]

$$h(x - \infty) = h_p(x) + \sum_{v \neq p} h_v(x) \tag{5}$$

of $h(x - \infty)$ into a sum of local heights such that $x \mapsto h_p(x)$ extends to a locally analytic function $\theta : X(\mathbf{Q}_p) \to \mathbf{Q}_p$ (in fact a sum of double Coleman integrals), and for $v \neq p$ the function $x \mapsto h_v(x)$ maps integral points in $X(\mathbf{Q})$ into a finite subset of $\mathbf{Q}_p$, and this set is trivial if v is a prime of good reduction. By assumption, the p-adic height can be expressed in terms of a bilinear map on $\mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^*$. Because θ and the set Υ of possible values of $\sum_{v \neq p} h_v(x)$ for integral $x \in X(\mathbf{Q})$ can be computed explicitly, this can be turned into a practical method for computing the integral points [BBM17].

Following [BD16], we construct a quadratic Chabauty pair by associating to points of X a mixed extension of p-adic Galois representations, and then taking the p-adic height in the sense of Nekovář [Nek93]. In [BD16, §5], a suitable G_L-representation $A_Z(b, x)$ is constructed for every $x \in X(L)$, where $L = \mathbf{Q}$ or $\mathbf{Q}_v$. It depends on the choice of a certain correspondence Z on X, which always exists when $\rho > 1$. By [BD16, Theorem 1.2], the height of $A_Z(b, x)$ is equal to the height pairing between two divisors given explicitly in terms of b, x and Z. In this paper, we work instead directly with the representation $A_Z(b, x)$, without determining the corresponding divisors. The advantage is that one does not need an explicit geometric description of Z, but only its cycle class.

Henceforth, h denotes Nekovář's p-adic height. Similar to (5), there is a local decomposition

$$h(A_Z(b, x)) = h_p(A_Z(b, x)) + \sum_{v \neq p} h_v(A_Z(b, x)),$$

where $x \mapsto h_p(A_Z(b, x))$ again extends to a locally analytic function $\theta : X(\mathbf{Q}_p) \to \mathbf{Q}_p$, and for $v \neq p$ the local heights $h_v(A_Z(b, x))$ take on a finite set of values Υ. By [BD16, §5], this gives a quadratic Chabauty pair (θ, Υ) whose pairing is h and whose endomorphism is the one induced by Z.

Suppose that X satisfies $r = g$ and $\rho > 1$, and that the p-adic closure of $\mathrm{J}(\mathbf{Q})$ has finite index in $\mathrm{J}(\mathbf{Q}_p)$. Note that these conditions are satisfied for many modular curves for which Chabauty–Coleman does not apply, see [Sik17], including $X_{\mathrm{s}}(13)$. Suppose that we have enough rational points $P_1, \dots, P_m$ to generate $\mathcal{E}$ as in §1.4. It follows from Lemma 1.5 that, if we can carry out the following steps explicitly, we have an explicit method for computing a finite subset of $X(\mathbf{Q}_p)$ containing $X(\mathbf{Q})$:

(i) Determine the set of values that $h_v(A_Z(b, x))$ can take for $x \in X(\mathbf{Q}_v)$ and $v \neq p$.
(ii) Expand the function $x \mapsto h_p(A_Z(b, x))$ into a p-adic power series on every residue disk.
(iii) Evaluate $h(A_Z(b, P_i))$ for $i = 1, \dots, m$.

In this paper, we say nothing about problem (i) since $X_{\mathrm{s}}(13)$, our main object of interest, has potentially good reduction everywhere, so that all local heights away from p are trivial. This also

reduces problem (iii) to problem (ii). Nevertheless, in the interest of future applications, we phrase much of the setup in greater generality than needed for the application to $X_{\mathrm{s}}(13)$.

1.6. **Explicit local p-adic heights at p.** The main contribution of this paper is to give an explicit algorithm for solving problem (ii). This is already done for hyperelliptic curves in [BD17], and we follow the general strategy used there. As in [Kim09, Had11], we emphasize the central role played by universal objects in neutral unipotent Tannakian categories. This approach allows us to make several aspects of [BD16] and [BD17] explicit in a conceptual way.

The definition of Nekovář's local height at p is in terms of p-adic Hodge theory. More precisely, let $M(x)$ denote the image of $A_Z(b,x)$ under Fontaine's $\mathbf{D}_{\mathrm{cris}}$-functor. Then $M(x)$ is a filtered ϕ-module, and to find $h_p(A_Z(b,x))$ it suffices to explicitly describe its Hodge filtration and its Frobenius action. It is shown in [BD17] that $M(x)$ can be described as the pullback along x of a certain universal connection $\mathcal{A}_Z$, which also carries a Frobenius structure. Our task is to find a sufficiently explicit description of both the Hodge filtration and the Frobenius structure on $\mathcal{A}_Z$. In [BD17], the Hodge filtration is computed using a universal property proved by Hadian [Had11], and we follow a similar strategy here. The explicit description of the Frobenius structure constitutes the key new result which makes our approach work. In the hyperelliptic situation, one gets a description in terms of Coleman integrals, but this crucially relies on the existence of the hyperelliptic involution [BD17, §6.6]. Here we characterise the Frobenius structure using a universal property, based on work of Kim [Kim09].

1.7. **Algorithmic remarks and applicability.** We note that while many of the constructions in this paper rely on deep results in p-adic Hodge theory, for a given curve, all of this can subsequently be translated into rather concrete linear algebra data which can be computed explicitly. For instance, instead of working with a correspondence Z explicitly, by the p-adic Lefschetz (1,1) theorem it is enough to work with the induced Tate class in $\mathrm{H}^1_{\mathrm{dR}}(X_{\mathbf{Q}_p}) \otimes \mathrm{H}^1_{\mathrm{dR}}(X_{\mathbf{Q}_p})$. In practice, we fix a basis of $\mathrm{H}^1_{\mathrm{dR}}(X_{\mathbf{Q}_p})$ and encode our Tate classes as matrices with respect to this basis. Computing the structure of $M(x)$ as a filtered ϕ-module boils down to computing two isomorphisms of $2g+2$-dimensional $\mathbf{Q}_p$-vector spaces

$$\mathbf{Q}_p \oplus \mathrm{H}^1_{\mathrm{dR}}(X_{\mathbf{Q}_p})^* \oplus \mathbf{Q}_p(1) \simeq M(x),$$

one of which respects the Hodge filtration, while the other one is Frobenius-equivariant. In practice, the universal properties discussed above give rise to explicit p-adic differential equations, which we solve using algorithms of the fourth author [Tui16, Tui17]. Our algorithms have been implemented in the computer algebra system `Magma` [BCP97] and can be found at [BDM+].

The results of this paper remain useful in somewhat less restrictive situations than the one considered above. For instance, as noted above, the condition that the curve has potentially good reduction everywhere is only used to give a particularly simple solution to problem (i) (and (iii)). Also, [BD16, §5.3] discusses an approach to computing a finite set containing $X(\mathbf{Q})$ when $r > g$, but $r + 1 - \rho < g$, and is similar to the one used here. For this approach one also needs to solve problem (ii), and our algorithm for its solution applies without change.

Moreover, recall that we have made the assumption that we have enough rational points available to span $\mathcal{E}$ as in §1.4. In practice, since $\rho > 1$, the algebra $K := \mathrm{End}(\mathrm{J}) \otimes \mathbf{Q}$ will be strictly larger than $\mathbf{Q}$ and, following [BD17], we can construct h so that it is K-equivariant. This means we can replace $\mathcal{E}$ by $\mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^* \otimes_{K \otimes \mathbf{Q}_p} \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^*$ in Lemma 1.5, which lowers the number of rational points required. We use this for $X = X_{\mathrm{s}}(13)$, so that we only need 4 rational points. If we have an algorithm to compute the p-adic height pairing between rational points on the Jacobian, and we have r independent rational points on J, we would only need one rational point on X, to serve as our base point.

1.8. **Outline.** In Section 2, we recall the salient points of Chabauty–Kim theory and in Section 3 we recall the definition of Nekovář's p-adic height and how it can be used to construct quadratic Chabauty pairs. Section 4 describes the computation of the Hodge filtration on a universal connection $\mathcal{A}_Z$, and

Section 5 describes the computation of its Frobenius structure. Both of these rely on universal properties and can be used to determine the structure of $A_Z(b,x)$ as a filtered ϕ-module. All aspects of this theory are then computed explicitly for $X = X_{\mathrm{s}}(13)$ in Section 6: We first show that the rank of $\mathrm{J}(\mathbf{Q})$ is exactly 3 and that X has potentially good reduction. We then run our algorithm for the local 17-adic height at $p = 17$ for two independent Tate classes coming from suitable correspondences, leading to two quadratic Chabauty pairs. As a consequence, we prove Theorem 1.1. The appendix contains a discussion of some concepts and results on unipotent neutral Tannakian categories used throughout the paper.

Acknowledgements. We are indebted to Minhyong Kim for proposing this project, and for his suggestions and encouragement. We thank René Schoof and Michael Stoll for comments on an earlier version of this paper. Balakrishnan is supported in part by NSF grant DMS-1702196, the Clare Boothe Luce Professorship (Henry Luce Foundation), and Simons Foundation grant #550023. Tuitman is a Postdoctoral Researcher of the Fund for Scientific Research FWO - Vlaanderen. Vonk is supported by a CRM/ISM Postdoctoral Scholarship at McGill University.

2. Chabauty-Kim and correspondences

In this section we briefly recall the main ideas in the non-abelian Chabauty method of Kim [Kim09]. We then recall some results from [BD16] which can be used to prove the finiteness of the set of rational points under certain assumptions. None of the results in this section are new.

In a letter to Faltings, Grothendieck proposed to study rational points on X through the geometric étale fundamental group $\pi_1^{\text{ét}}(\overline{X}, b)$ of X with base point b. More precisely, he conjectured that the map

$$X(\mathbf{Q}) \longrightarrow \mathrm{H}^1\left(G_{\mathbf{Q}}, \pi_1^{\text{ét}}(\overline{X}, b)\right),$$

given by associating to $x \in X(\mathbf{Q})$ the étale path torsor $\pi_1^{\text{ét}}(\overline{X}; b, x)$, should be an isomorphism. Unfortunately, there seems to a lack of readily available extra structure on the target, which makes it difficult to study directly. However, one can try instead to work with a suitable quotient of $\pi_1^{\text{ét}}(\overline{X}, b)$, where "suitable" depends on the properties of the curve in question. Most techniques for studying $X(\mathbf{Q})$ can be phrased in this language. Chabauty–Coleman, finite cover descent (see for instance [BS09]) and elliptic curve Chabauty [FW99, Bru03] rely on *abelian* quotients, whereas Chabauty–Kim, discussed below, uses *unipotent* quotients. Following [BD16] we will construct quadratic Chabauty pairs for a class of curves including $X_{\mathrm{s}}(13)$ from the simplest non-abelian unipotent quotient when $r = g$ and $\rho > 1$.

2.1. **The Chabauty-Kim method.** Let $V := \mathrm{H}^1_{\text{ét}}(\overline{X}, \mathbf{Q}_p)^*$, and $V_{\mathrm{dR}} := \mathrm{H}^1_{\mathrm{dR}}(X_{\mathbf{Q}_p})^*$, viewed as a filtered vector space with the dual filtration to the Hodge filtration, so that there is an isomorphism $V_{\mathrm{dR}}/\operatorname{Fil}^0 \simeq \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^*$. Bloch–Kato show there is an isomorphism $\mathrm{H}^1_{\mathrm{f}}(G_p, V) \simeq V_{\mathrm{dR}}/\operatorname{Fil}^0$, and it follows from [BK90, 3.10.1] that there is a commutative diagram

(6)
$$\begin{array}{ccccc}
X(\mathbf{Q}) & \longrightarrow & X(\mathbf{Q}_p) & \xrightarrow{\mathrm{AJ_b}} & \\
\downarrow & & \downarrow & & \\
\mathrm{J}(\mathbf{Q}) & \longrightarrow & \mathrm{J}(\mathbf{Q}_p) & \xrightarrow{\log} & \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^* \\
\downarrow{\scriptstyle \kappa} & & \downarrow{\scriptstyle \kappa_p} & & \downarrow{\scriptstyle \wr} \\
\mathrm{H}^1_{\mathrm{f}}(G_T, V) & \xrightarrow{\mathrm{loc}_p} & \mathrm{H}^1_{\mathrm{f}}(G_p, V) & \xrightarrow{\simeq} & V_{\mathrm{dR}}/\operatorname{Fil}^0
\end{array}$$

extending the Chabauty diagram (2). Here κ and κ_p map a point to its Kummer class, $\mathrm{H}^1_{\mathrm{f}}(G_p, V)$ is the subspace of $\mathrm{H}^1(G_p, V)$ consisting of crystalline torsors [BK90, (3.7.2)], and $\mathrm{H}^1_{\mathrm{f}}(G_T, V) = \mathrm{loc}_p^{-1}\,\mathrm{H}^1_{\mathrm{f}}(G_p, V)$.

The idea of the Chabauty–Kim method is essentially that, if we cut out the middle row of this diagram, we obtain something amenable to generalisation. Namely, for each n we obtain:

$$\begin{array}{ccccc} X(\mathbf{Q}) & \longrightarrow & X(\mathbf{Q}_p) & & \\ \downarrow{\scriptstyle j_n^{\text{ét}}} & & \downarrow{\scriptstyle j_{n,p}^{\text{ét}}} & \searrow^{j_n^{\mathrm{dR}}} & \\ \mathrm{Sel}(\mathrm{U}_n) & \xrightarrow{\mathrm{loc}_{n,p}} & \mathrm{H}^1_{\mathrm{f}}(G_p, \mathrm{U}_n^{\text{ét}}) & \xrightarrow{\mathbf{D}} & \mathrm{U}_n^{\mathrm{dR}} / \mathrm{Fil}^0. \end{array} \tag{7}$$

We now define the objects in this diagram precisely, following [Kim09]. Let $\mathrm{U}_n^{\text{ét}} := \mathrm{U}_n^{\text{ét}}(b)$ denote the maximal n-unipotent quotient of the $\mathbf{Q}_p$-étale fundamental group of $\overline{X}$ with base point b. This is a finite-dimensional unipotent group over $\mathbf{Q}_p$ with a continuous action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, which contains the maximal n-unipotent pro-p quotient of $\pi_1^{\text{ét}}(\overline{X}, b)$ as a lattice. In this paper, we only need $n = 1$ or 2. We have $\mathrm{U}_1^{\text{ét}} = V$, and $\mathrm{U}_2^{\text{ét}}$ is a central extension

$$1 \longrightarrow \mathrm{Coker}\left(\mathbf{Q}_p(1) \xrightarrow{\cup^*} \wedge^2 V\right) \longrightarrow \mathrm{U}_2 \longrightarrow V \longrightarrow 1. \tag{8}$$

We obtain for any $x \in X(\mathbf{Q})$ a path torsor $\mathrm{U}_n^{\text{ét}}(b, x)$, see §A. This gives rise to a map

$$j_n^{\text{ét}} : X(\mathbf{Q}) \longrightarrow \mathrm{H}^1(G_T, \mathrm{U}_n^{\text{ét}}),\ x \mapsto \mathrm{U}_n^{\text{ét}}(b, x),$$

as well as local versions $j_{n,v}^{\text{ét}}$ for any finite place v. We obtain the commutative diagram

$$\begin{array}{ccc} X(\mathbf{Q}) & \longrightarrow & \prod_{v\in T} X(\mathbf{Q}_v) \\ \downarrow{\scriptstyle j_n^{\text{ét}}} & & \downarrow{\scriptstyle \prod j_{n,v}^{\text{ét}}} \\ \mathrm{H}^1(G_T, \mathrm{U}_n^{\text{ét}}) & \xrightarrow{\prod \mathrm{loc}_{n,v}} & \prod_{v\in T} \mathrm{H}^1(G_v, \mathrm{U}_n^{\text{ét}}). \end{array}$$

By [Ols11], we have $j_{n,p}^{\text{ét}}(X(\mathbf{Q}_p)) \subset \mathrm{H}^1_{\mathrm{f}}(G_p, \mathrm{U}_n^{\text{ét}})$. It is shown in [Kim05] that $\mathrm{H}^1(G_p, \mathrm{U}_n^{\text{ét}})$ and $\mathrm{H}^1(G_T, \mathrm{U}_n^{\text{ét}})$ are represented by algebraic varieties over $\mathbf{Q}_p$. By [Kim09, p. 119], $\mathrm{H}^1_{\mathrm{f}}(G_p, \mathrm{U}_n^{\text{ét}})$ is represented by a subvariety of $\mathrm{H}^1(G_p, \mathrm{U}_n^{\text{ét}})$, and the analogous statement holds for $\mathrm{H}^1_{\mathrm{f}}(G_T, \mathrm{U}_n^{\text{ét}})$. Similar to classical Selmer groups, we add local conditions and define the *Selmer variety* $\mathrm{Sel}(\mathrm{U}_n)$ to be the subvariety of $\mathrm{H}^1_{\mathrm{f}}(G_T, \mathrm{U}_n^{\text{ét}})$ consisting of all classes

$$c \in \bigcap_{v\in T_0} \mathrm{loc}_{n,v}^{-1}(j_{n,v}^{\text{ét}}(X(\mathbf{Q}_v)))$$

whose projection to $\mathrm{H}^1_f(G_T, V)$ lies in the image of $\mathrm{J}(\mathbf{Q}) \otimes \mathbf{Q}_p$, see diagram (6) above. See [BD16, Remark 2.3] for a discussion how our definition relates to other definitions of Selmer varieties (and schemes) in the literature.

Remark 2.1. Since $X = X_{\mathrm{s}}(13)$ has potentially good reduction everywhere, see Corollary 6.7, the local conditions at $v \neq p$ are vacuous for this example, and the Selmer variety is simply $\mathrm{H}^1_{\mathrm{f}}(G_T, \mathrm{U}_n)$.

Finally, we define the objects on the right side of diagram (7). Let L be a field of characteristic zero. Deligne [Del89, Section 10] constructs the *de Rham fundamental group*

$$\pi_1^{\mathrm{dR}}(X_L, b),$$

a pro-unipotent group over L, defined as the Tannakian fundamental group of the category $\mathcal{C}^{\mathrm{dR}}(X_L)$ of unipotent vector bundles with flat connection on X with respect to the fibre functor b^*. When there is no risk of confusion, we drop the subscript L. Define $\mathrm{U}_n^{\mathrm{dR}}(b)$ to be the maximal n-unipotent quotient of $\pi_1^{\mathrm{dR}}(X, b)$, along with path torsors $\mathrm{U}_n^{\mathrm{dR}}(b, x)$ for all $x \in X(L)$. These have the structure of filtered

ϕ-modules. Kim shows [Kim09] that the isomorphism classes of $\mathrm{U}_n^{\mathrm{dR}}$-torsors in the category of filtered ϕ-modules are naturally classified by the scheme $\mathrm{U}_n^{\mathrm{dR}} / \mathrm{Fil}^0$. Hence, we get a tower of maps

$$j_n^{\mathrm{dR}} : X(\mathbf{Q}_p) \longrightarrow \mathrm{U}_n^{\mathrm{dR}} / \mathrm{Fil}^0, \ x \mapsto \mathrm{U}_n^{\mathrm{dR}}(b, x).$$

More generally, for any Galois stable quotient U of $\mathrm{U}_n^{\text{ét}}$, we have a diagram similar to (7) involving $\mathrm{U}^{\mathrm{dR}} := \mathbf{D}_{\mathrm{cris}}(\mathrm{U})$, where $\mathrm{Sel}(\mathrm{U})$ and the corresponding maps $j_{\mathrm{U}}^{\text{ét}}, j_{\mathrm{U}}^{\mathrm{dR}}$ and $\mathrm{loc}_{\mathrm{U},p}$ are defined in the same way. We then have that $X(\mathbf{Q})$ is contained in the subset

$$X(\mathbf{Q}_p)_{\mathrm{U}} := (j_{\mathrm{U},p}^{\text{ét}})^{-1} (\mathrm{loc}_{\mathrm{U},p} \mathrm{Sel}(\mathrm{U})) \subset X(\mathbf{Q}_p).$$

When $\mathrm{U} = \mathrm{U}_n$, we write $X(\mathbf{Q}_p)_n$ for this subset, its elements are called *weakly global points*. We have

$$X(\mathbf{Q}) \subset \ldots \subset X(\mathbf{Q}_p)_n \subset X(\mathbf{Q}_p)_{n-1} \subset \ldots \subset X(\mathbf{Q}_p)_2 \subset X(\mathbf{Q}_p)_1 \subset X(\mathbf{Q}_p).$$

2.2. **Diophantine finiteness.** In [Kim09], Kim showed how the set-up of Chabauty's theorem may be generalised to diagram (7). The sets in the bottom row have the structure of $\mathbf{Q}_p$-points of algebraic varieties, in such a way that the morphisms $\mathrm{loc}_{n,p}$ and $\mathbf{D}$ are morphisms of schemes (and $\mathbf{D}$ is an isomorphism). The analogue of the analytic properties of AJ_{b} is the theorem that j_n^{dR} has Zariski dense image [Kim09, Theorem 1] and is given by a power series on each residue disk. The analogue of Chabauty's $r < g$ condition is non-density of the localisation map $\mathrm{loc}_{\mathrm{U}_n,p}$. As in the classical case, this gives the following theorem.

Theorem 2.2 (Kim)**.** *Suppose* $\mathrm{loc}_{\mathrm{U},p}$ *is non-dominant. Then* $X(\mathbf{Q}_p)_{\mathrm{U}}$ *is finite.*

Kim [Kim09, §3] showed that non-density of $\mathrm{loc}_{\mathrm{U},p}$ (and hence finiteness of $X(\mathbf{Q}_p)_{\mathrm{U}}$) is implied by various conjectures on the size of unramified Galois cohomology groups (for example by the Beilinson–Bloch–Kato conjectures) but is hard to prove unconditionally. One instance where the relevant Galois cohomology groups can be understood by Iwasawa theoretic methods is when the Jacobian of X has CM. This was used by Coates and Kim [CK10] to prove eventual finiteness of weakly global points. Recently, Ellenberg and Hast [EH17] prove, using similar techniques, that the class of curves admitting an étale cover all of whose twists have eventually finite sets of weakly global points includes all solvable Galois covers of $\mathbf{P}^1$. In this article the Galois cohomological input needed is of a much more elementary nature. The following result was proved by Balakrishnan–Dogra [BD16, Lemma 3].

Lemma 2.3 (Balakrishnan–Dogra)**.** *Recall that* $r = \mathrm{rk}\, J(\mathbf{Q})$ *and* $\rho = \rho(J_{\mathbf{Q}}) = \mathrm{rk}\, \mathrm{NS}(J_{\mathbf{Q}})$*. Suppose*

$$r < g + \rho - 1.$$

Then $X(\mathbf{Q}_p)_2$ *is finite.*

The idea of the proof of this lemma is as follows. As the map $\mathrm{loc}_{2,p}$ is algebraic, it suffices by Theorem 2.2 to construct a Galois-stable quotient U of U_2 for which $\dim \mathrm{H}^1_{\mathrm{f}}(G_T, \mathrm{U}) < \dim \mathrm{H}^1_{\mathrm{f}}(G_p, \mathrm{U})$, since $X(\mathbf{Q}_p)_2 \subset X(\mathbf{Q}_p)_{\mathrm{U}}$. We can push out (8) to construct a quotient U of U_2 which is an extension

$$1 \longrightarrow \mathbf{Q}_p(1)^{\oplus(\rho-1)} \longrightarrow \mathrm{U} \longrightarrow V \longrightarrow 1.$$

Using the six-term exact sequence in nonabelian cohomology and some p-adic Hodge theory, one shows $\dim \mathrm{H}^1_{\mathrm{f}}(G_T, \mathrm{U}) \leq r$, whereas $\dim \mathrm{H}^1_{\mathrm{f}}(G_p, \mathrm{U}) = g + \rho - 1$.

2.3. **Quotients of fundamental groups via correspondences.** Lemma 2.3, as well as the results of [CK10, EH17] where finiteness is proved unconditionally in certain cases, say nothing about how to actually *determine* $X(\mathbf{Q}_p)_2$ or $X(\mathbf{Q})$ in practice. In [BD16, BD17], the two first-named authors construct a suitable intermediate quotient U between U_2 and V that is non-abelian, but small enough to make explicit computations possible. Working with such quotients U, rather than directly with U_2, may be thought of as a non-abelian analogue of passing to a nice quotient of the Jacobian, as, for

instance, in the work of Mazur [Maz77] and Merel [Mer96]. Lemma 2.3 was deduced from the finiteness of such a set $X(\mathbf{Q}_p)_{\mathrm{U}}$, and it is these sets which will be computed explicitly in what follows.

Denoting by τ the canonical involution $(x_1, x_2) \mapsto (x_2, x_1)$ on $X \times X$, we say that a correspondence $Z \in \mathrm{Pic}(X \times X)$ is *symmetric* if there are $Z_1, Z_2 \in \mathrm{Pic}(X)$ such that

$$\tau_* Z = Z + \pi_1^* Z_1 + \pi_2^* Z_2,$$

where π_1, π_2 are the canonical projections $X \times X \to X$. We say that Z is a *nice* correspondence if Z is nontrivial, symmetric, and ξ_Z has trace 0, where $\xi_Z \in \mathrm{H}^1(X) \otimes \mathrm{H}^1(X)(1) \simeq \mathrm{End}\,\mathrm{H}^1(X)$ is the cycle class and $\mathrm{H}^*(X)$ is any Weil cohomology theory with coefficient field L of characteristic zero.

Lemma 2.4. *Suppose that* J *is absolutely simple and let* $Z \in \mathrm{Pic}(X \times X)$ *be a symmetric correspondence. Then the class associated to* Z *lies in the subspace*

$$\bigwedge^2 \mathrm{H}^1(X)(1) \subset \mathrm{H}^1(X) \otimes \mathrm{H}^1(X)(1).$$

Moreover, Z *is nice if and only if the image of this class in* $\mathrm{H}^2(X)(1)$ *under the cup product is zero.*

Proof. It follows from [BL04, Proposition 11.5.3], whose proof remains valid over any base field, that a correspondence is symmetric if and only if its induced endomorphism of J is fixed by the Rosati involution. By [Mum70, §IV.20] the subspace of $\mathrm{End}(\mathrm{J}) \otimes \mathbf{Q}$ fixed by the Rosati involution is isomorphic to $\mathrm{NS}(\mathrm{J}) \otimes \mathbf{Q}$, so we find that Z induces an element of $\mathrm{NS}(\mathrm{J})$. Hence the class associated to Z lies in $\mathrm{H}^2(\mathrm{J})(1) = \wedge^2 \mathrm{H}^1(X)(1)$.

The second statement is a consequence of the observation that the trace of ξ_Z as a linear operator on $\mathrm{H}^1(X)$ is equal to the composite of the cup product and the trace isomorphism

$$\mathrm{H}^1(X) \otimes \mathrm{H}^1(X)(1) \longrightarrow \mathrm{H}^2(X)(1) \simeq L. \qquad \square$$

We now define quotients U_Z of U_2 attached to the choice of a nice correspondence Z on X. These underlie the proof of Lemma 2.3, and play a crucial role in our determination of $X_{\mathrm{s}}(13)(\mathbf{Q})$. By Lemma 2.4, if Z is a nice correspondence on X, we obtain a homomorphism

$$c_Z : \mathbf{Q}_p(-1) \longrightarrow \mathrm{Ker}\left(\wedge^2 \mathrm{H}^1_{\text{ét}}(X_{\overline{\mathbf{Q}}}, \mathbf{Q}_p) \xrightarrow{\cup} \mathrm{H}^2(X_{\overline{\mathbf{Q}}}, \mathbf{Q}_p)\right),$$

and hence by (8), we may form the quotient $\mathrm{U}_Z := \mathrm{U}_2 / \mathrm{Ker}(c_Z^*)$, which sits in an exact sequence

$$1 \to \mathbf{Q}_p(1) \to \mathrm{U}_Z \to V \to 1.$$

Remark 2.5. In the computations of this paper, we never work with nice correspondences directly, but rather with their images in $\mathrm{H}^1_{\mathrm{dR}}(X) \otimes \mathrm{H}^1_{\mathrm{dR}}(X)(1)$. In fact, we can carry out these computations for quotients corresponding in the same way to more general Tate classes $\mathrm{H}^1_{\mathrm{dR}}(X) \otimes \mathrm{H}^1_{\mathrm{dR}}(X)$ which come from a nice $Z \in \mathrm{Pic}(X \times X) \otimes \mathbf{Q}_p$, for which we extend the notion of a nice correspondence in the obvious way. For notational convenience, we denote a class obtained in this way by Z as well.

3. Height functions on the Selmer variety

In this section we recall Nekovář's theory of p-adic height functions [Nek93] and summarise some results of [BD16] relating p-adic heights to Selmer varieties and leading to a construction of quadratic Chabauty pairs when $r = g$ and $\rho > 1$.

3.1. Nekovář's p-adic height functions.

We start by recalling some definitions from the theory of p-adic heights due to Nekovář [Nek93]. The necessary background from p-adic Hodge theory can be found in [Nek93, Section 1]. For a wide class of p-adic Galois representations V, Nekovář [Nek93, Section 2] constructs a continuous bilinear pairing

$$h : \mathrm{H}^1_{\mathrm{f}}(G_T, V) \times \mathrm{H}^1_{\mathrm{f}}(G_T, V^*(1)) \longrightarrow \mathbf{Q}_p\,. \tag{9}$$

This global height pairing depends only on the choice of

- a continuous idèle class character $\chi : \mathbf{A}_{\mathbf{Q}}^{\times}/\,\mathbf{Q}^{\times} \longrightarrow \mathbf{Q}_p$,
- a splitting $s : V_{\mathrm{dR}}/\operatorname{Fil}^0 V_{\mathrm{dR}} \longrightarrow V_{\mathrm{dR}}$ of the Hodge filtration, where $V_{\mathrm{dR}} = \mathbf{D}_{\mathrm{cris}}(V)$.

Henceforth, we fix such choices once and for all. We will only consider $V = \mathrm{H}^1_{\text{ét}}(X_{\overline{\mathbf{Q}}}, \mathbf{Q}_p)^*$, and specialise immediately to this case for simplicity, so that $V_{\mathrm{dR}} = \mathrm{H}^1_{\mathrm{dR}}(X_{\mathbf{Q}_p})^*$.

The global p-adic height pairing h decomposes as the sum of local pairings h_v, for every non-archimedean place v of $\mathbf{Q}$, as explained in [Nek93, Section 4]. As in the classical decomposition of the height pairing, the local height functions do not define a bilinear pairing, but rather a bi-additive function on a set of equivalence classes of mixed extensions, which we now explain. In the particular example of $X = X_{\mathrm{s}}(13)$, only the local height h_p is of importance. Recall that $T = T_0 \cup \{p\}$, where T_0 is the set of primes of bad reduction of X.

Definition 3.1. *Let G be the Galois group G_T or G_v, for $v \in T$. Define $\mathcal{M}(G; \mathbf{Q}_p, V, \mathbf{Q}_p(1))$ to be the category of mixed extensions with graded pieces $\mathbf{Q}_p, V$, and $\mathbf{Q}_p(1)$, with objects $(M, M_\bullet, \psi_\bullet)$, where*

- *M is a $\mathbf{Q}_p$-representation of G,*
- *$M_\bullet$ is a G-stable filtration $M = M_0 \supset M_1 \supset M_2 \supset M_3 = 0$,*
- *$\psi_\bullet$ are isomorphisms of G-representations*

$$\begin{cases} \psi_0 : M_0/M_1 & \xrightarrow{\sim} & \mathbf{Q}_p, \\ \psi_1 : M_1/M_2 & \xrightarrow{\sim} & V, \\ \psi_2 : M_2/M_3 & \xrightarrow{\sim} & \mathbf{Q}_p(1), \end{cases}$$

and whose morphisms

$$(M, M_\bullet, \psi_\bullet) \longrightarrow (M', M'_\bullet, \psi'_\bullet)$$

are morphisms $M \to M'$ of representations which respect the filtrations and commute with the isomorphisms ψ_i and ψ'_i. Let $\mathrm{M}(G; \mathbf{Q}_p, V, \mathbf{Q}_p(1))$ denote the set of isomorphism classes of objects.

When $G = G_T$ or G_p, we denote by $\mathcal{M}_{\mathrm{f}}(G; \mathbf{Q}_p, V, \mathbf{Q}_p(1))$ the full subcategory of $\mathcal{M}(G; \mathbf{Q}_p, V, \mathbf{Q}_p(1))$ consisting of representations which are crystalline at p, and similarly define $\mathrm{M}_{\mathrm{f}}(G; \mathbf{Q}_p, V, \mathbf{Q}_p(1))$.

The set $\mathrm{M}_{\mathrm{f}}(G_T; \mathbf{Q}_p, V, \mathbf{Q}_p(1))$ is equipped with two natural surjective homomorphisms

$$\begin{array}{rccll} \pi_1 : & \mathrm{M}_{\mathrm{f}}(G_T; \mathbf{Q}_p, V, \mathbf{Q}_p(1)) & \longrightarrow & \mathrm{H}^1_{\mathrm{f}}(G_T, V)\ , & M \mapsto [M/M_2], \\ \pi_2 : & \mathrm{M}_{\mathrm{f}}(G_T; \mathbf{Q}_p, V, \mathbf{Q}_p(1)) & \longrightarrow & \mathrm{Ext}^1_{G_T,\mathrm{f}}(V, \mathbf{Q}_p(1))\ , & M \mapsto [M_1]. \end{array}$$

(and similarly for the groups G_v, for $v \in T$). Throughout this paper, we implicitly identify $\mathrm{H}^1_{\mathrm{f}}(G_T, V)$ and $\mathrm{H}^1_{\mathrm{f}}(G_T, V^*(1))$ with the groups $\mathrm{Ext}^1_{G_T,\mathrm{f}}(\mathbf{Q}_p, V)$ and $\mathrm{Ext}^1_{G_T,\mathrm{f}}(V, \mathbf{Q}_p(1))$ respectively, where the subscript f denotes those extensions which are crystalline at p. Via Poincaré duality, we may view both $\pi_1(M)$ and $\pi_2(M)$ as elements of $H^1_f(G_T, V)$. We say M is a *mixed extension of $\pi_1(M)$ and $\pi_2(M)$*.

Nekovář's global height pairing (9) decomposes as a sum of local heights in the following sense. There exist functions h_p and h_v for every finite place $v \neq p$:

$$\begin{array}{rccc} h_p : & \mathrm{M}_{\mathrm{f}}(G_p; \mathbf{Q}_p, V, \mathbf{Q}_p(1)) & \longrightarrow & \mathbf{Q}_p \\ h_v : & \mathrm{M}(G_v; \mathbf{Q}_p, V, \mathbf{Q}_p(1)) & \longrightarrow & \mathbf{Q}_p \end{array}$$

such that $h = \sum_v h_v$, where h is viewed by abuse of notation as the composite function

$$\mathrm{M}_{\mathrm{f}}(G_T; \mathbf{Q}_p, V, \mathbf{Q}_p(1)) \xrightarrow{(\pi_1,\pi_2)} \mathrm{H}^1_{\mathrm{f}}(G_T, V) \times \mathrm{Ext}^1_{G_T,\mathrm{f}}(V, \mathbf{Q}_p(1)) \xrightarrow{h} \mathbf{Q}_p\,.$$

Note that (π_1, π_2) is surjective by [Nek93, §4.4]. Unlike the global height h, the local heights h_v do not factor through the map analogous to (π_1, π_2). We now define the functions h_v for $v \neq p$ and $v = p$, and refer to Nekovář [Nek93, Section 4] for more details.

3.2. **The local height away from p.** We recall the definition of the local height away from p, see [Nek93, §4.6]. By the weight-monodromy conjecture for curves proved by Raynaud [Ray94], we have $\mathrm{H}^1(G_v, V) = 0$. This implies that a mixed extension M in $\mathrm{M_f}(G_v; \mathbf{Q}_p, V, \mathbf{Q}_p(1))$ splits as $M \simeq V \oplus N$, where N is an extension of $\mathbf{Q}_p$ by $\mathbf{Q}_p(1)$. We obtain a class $[N] \in \mathrm{H}^1(G_v, \mathbf{Q}_p(1))$. Via Kummer theory [Nek93, §1.12] the local component $\chi_v : \mathbf{Q}_v^\times \longrightarrow \mathbf{Q}_p$ gives a map

$$\chi_v : \mathrm{H}^1(G_v, \mathbf{Q}_p(1)) \simeq \mathbf{Q}_v^\times \mathbin{\widehat{\otimes}} \mathbf{Q}_p \longrightarrow \mathbf{Q}_p,$$

The local height at v is now defined as

$$h_v(M) := \chi_v([N]).$$

When M is unramified at v, the local height automatically vanishes. More generally, we have:

Lemma 3.2. *Let $v \neq p$, and let $M \in \mathrm{M}(G_v; \mathbf{Q}_p, V, \mathbf{Q}_p(1))$ be a mixed extension. Assume that M is potentially unramified, then $h_v(M) = 0$.*

Proof. Suppose that $K_v/\mathbf{Q}_v$ is a finite Galois extension such that the action of G_{K_v} on M is unramified. The inflation-restriction sequence attached to this subgroup gives an exact sequence

$$0 \longrightarrow \mathrm{H}^1(A, \mathbf{Q}_p(1)^{G_{K_v}}) \longrightarrow \mathrm{H}^1(G_v, \mathbf{Q}_p(1)) \xrightarrow{\mathrm{res}} \mathrm{H}^1(G_{K_v}, \mathbf{Q}_p(1)),$$

where $A = G_v/G_{K_v}$ is a finite group. Write $M \simeq V \oplus N$, where N is an extension of $\mathbf{Q}_p$ by $\mathbf{Q}_p(1)$. Then by assumption, we have that the class of N in $\mathrm{H}^1(G_{K_v}, \mathbf{Q}_p(1))$ is trivial. On the other hand, the restriction map res is injective, since $\mathbf{Q}_p(1)^{G_{K_v}} = 0$. This shows that the class of N in $\mathrm{H}^1(G_v, \mathbf{Q}_p(1))$ is trivial, and in particular that $h_v(M) = 0$. □

3.3. **The local height at $v = p$.** Given a mixed extension $M_{\text{ét}} \in \mathrm{M_f}(G_p; \mathbf{Q}_p, V, \mathbf{Q}_p(1))$, the definition of its local height at p is in terms of $M_{\mathrm{dR}} := \mathbf{D}_{\mathrm{cris}}(M_{\text{ét}})$, see [Nek93, §4.7]. The module M_{dR} inherits a structure of *mixed extension* similar to that of $M_{\text{ét}}$, which we formalise in Definition 3.4.

Definition 3.3. *A filtered ϕ-module is a finite-dimensional $\mathbf{Q}_p$-vector space W equipped with an exhaustive and separated decreasing filtration Fil^i and an automorphism $\phi = \phi_W$.*

Really, we are only interested in *admissible* filtered ϕ-modules, but since we will only consider iterated extensions of filtered ϕ-modules which are admissible, and any extension of two admissible filtered ϕ-modules is admissible, we will ignore this distinction.

For any filtered ϕ-module W for which $W^{\phi=1} = 0$, we have (see [Nek93, §3.1]) an isomorphism

$$\mathrm{Ext}^1_{\mathrm{Fil},\phi}(\mathbf{Q}_p, W) \simeq W/\mathrm{Fil}^0, \tag{10}$$

Explicitly, the map from the Ext-group to W/Fil^0 is defined as follows. Given an extension

$$0 \longrightarrow W \longrightarrow E \longrightarrow \mathbf{Q}_p \longrightarrow 0,$$

one chooses a splitting $s^\phi : \mathbf{Q}_p \to E$ which is ϕ-equivariant, and a splitting s^{Fil} which respects the filtration. Their difference gives an element of W. Since $W^{\phi=1} = 0$, the splitting s^ϕ is unique, whereas s^{Fil} is only determined up to an element of $\mathrm{Fil}^0 W$. Hence the element $s^\phi - s^{\mathrm{Fil}} \in W \mod \mathrm{Fil}^0$ is independent of choices. We leave the construction of the inverse map to the reader.

Definition 3.4. *Let V be as above, and let $V_{\mathrm{dR}} = \mathbf{D}_{\mathrm{cris}}(V)$. Define $\mathcal{M}_{\mathrm{Fil},\phi}(\mathbf{Q}_p, V, \mathbf{Q}_p(1))$ to be the category of mixed extensions of filtered ϕ-modules, whose objects are tuples $(M, M_\bullet, \psi_\bullet)$ where*

- *M is a filtered ϕ-module,*
- *$M_\bullet$ is a filtration by sub-filtered ϕ-modules $M = M_0 \supset M_1 \supset M_2 \supset M_3 = 0$,*

- *$\psi_\bullet$ are isomorphisms of filtered ϕ-modules*

$$\begin{cases} \psi_0 : M_0/M_1 & \xrightarrow{\sim} & \mathbf{Q}_p \\ \psi_1 : M_1/M_2 & \xrightarrow{\sim} & V_{\mathrm{dR}} \\ \psi_2 : M_2/M_3 & \xrightarrow{\sim} & \mathbf{Q}_p(1) \end{cases}$$

and whose morphisms are morphisms of filtered ϕ-modules which in addition respect the filtrations $M_\bullet$ and commute with the isomorphisms ψ_i and ψ_i'. Let $\mathrm{M}_{\mathrm{Fil},\phi}(\mathbf{Q}_p, V, \mathbf{Q}_p(1))$ denote the set of isomorphism classes of objects.

The structure of a mixed extension of filtered ϕ-modules on $M_{\mathrm{dR}} = \mathbf{D}_{\mathrm{cris}}(M_{\text{ét}})$ naturally allows us to define extensions $E_1(M)$ and $E_2(M)$ by

$$E_1(M) := M_{\mathrm{dR}}/\,\mathbf{Q}_p(1), \qquad E_2(M) := \mathrm{Ker}(M_{\mathrm{dR}} \to \mathbf{Q}_p), \tag{11}$$

compare with the definition of π_1 and π_2 above. For simplicity we will sometimes write these as E_1 and E_2. We have a short exact sequence

$$0 \longrightarrow \mathbf{Q}_p(1) \longrightarrow E_2/\,\mathrm{Fil}^0 \longrightarrow V_{\mathrm{dR}}/\,\mathrm{Fil}^0 \longrightarrow 0. \tag{12}$$

The image of the extension class $[M] \in \mathrm{H}^1_{\mathrm{f}}(G_p, E_2) \simeq E_2/\,\mathrm{Fil}^0$ in the group $V_{\mathrm{dR}}/\,\mathrm{Fil}^0 \simeq \mathrm{H}^1_{\mathrm{f}}(G_p, V_{\mathrm{dR}})$ is exactly the extension class $[E_1]$. We define δ to be the composite map

$$\delta \;:\; V_{\mathrm{dR}}/\,\mathrm{Fil}^0 \xrightarrow{s} V_{\mathrm{dR}} \longrightarrow E_2 \longrightarrow E_2/\,\mathrm{Fil}^0,$$

where the homomorphism $V_{\mathrm{dR}} \to E_2$ is the unique Frobenius-equivariant splitting of

$$0 \longrightarrow \mathbf{Q}_p(1) \longrightarrow E_2 \longrightarrow V_{\mathrm{dR}} \longrightarrow 0,$$

and the last map is just the canonical surjection. By construction, $[M]$ and $\delta([E_1])$ have the same image in $V_{\mathrm{dR}}/\,\mathrm{Fil}^0$, hence via the exact sequence (12) their difference defines an element of $\mathbf{Q}_p(1)$. The filtered ϕ-module $\mathbf{Q}_p(1)$ is isomorphic to $\mathrm{H}^1_{\mathrm{f}}(G_p, \mathbf{Q}_p(1))$ via (10), so we may think of $[M] - \delta([E_1])$ as an element of $\mathrm{H}^1_{\mathrm{f}}(G_p, \mathbf{Q}_p(1))$. The local component $\chi_p : \mathbf{Q}_p^\times \longrightarrow \mathbf{Q}_p$ gives rise to a map

$$\chi_p : \mathrm{H}^1_{\mathrm{f}}(G_p, \mathbf{Q}_p(1)) \simeq \mathbf{Z}_p^\times \mathbin{\widehat{\otimes}} \mathbf{Q}_p \longrightarrow \mathbf{Q}_p$$

where the isomorphism follows from Kummer theory. This allows us to define

$$h_p(M) := \chi_p\left([M] - \delta([E_1])\right). \tag{13}$$

For the practical determination of rational points, it will be necessary to make this more explicit. To do so, it is convenient to introduce some notation for filtered ϕ-modules M in $\mathrm{M}_{\mathrm{Fil},\phi}(\mathbf{Q}_p, V, \mathbf{Q}_p(1))$. The splitting s of $\mathrm{Fil}^0 V_{\mathrm{dR}}$ defines idempotents $s_1, s_2 : V_{\mathrm{dR}} \longrightarrow V_{\mathrm{dR}}$ projecting onto the $s(V_{\mathrm{dR}}/\,\mathrm{Fil}^0)$ and Fil^0 components respectively. Suppose we are given a vector space splitting

$$s_0 : \mathbf{Q}_p \oplus V_{\mathrm{dR}} \oplus \mathbf{Q}_p(1) \xrightarrow{\sim} M.$$

The split mixed extension $\mathbf{Q}_p \oplus V_{\mathrm{dR}} \oplus \mathbf{Q}_p(1)$ has the structure of a filtered ϕ-module as a direct sum. Choose two further splittings

$$\begin{array}{rcccc} s^\phi & : & \mathbf{Q}_p \oplus V_{\mathrm{dR}} \oplus \mathbf{Q}_p(1) & \xrightarrow{\sim} & M \\ s^{\mathrm{Fil}} & : & \mathbf{Q}_p \oplus V_{\mathrm{dR}} \oplus \mathbf{Q}_p(1) & \xrightarrow{\sim} & M \end{array}$$

where s^ϕ is Frobenius equivariant, and s^{Fil} respects the filtrations. Note that the choice of s^ϕ is unique, whereas the choice of s^{Fil} is not. Suppose we have chosen bases for $\mathbf{Q}_p, V_{\mathrm{dR}}$, and $\mathbf{Q}_p(1)$ such that with respect to these bases, we have

$$s_0^{-1} \circ s^\phi = \begin{pmatrix} 1 & 0 & 0 \\ \boldsymbol{\alpha}_\phi & 1 & 0 \\ \gamma_\phi & \boldsymbol{\beta}_\phi^{\intercal} & 1 \end{pmatrix} \qquad s_0^{-1} \circ s^{\mathrm{Fil}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \gamma_{\mathrm{Fil}} & \boldsymbol{\beta}_{\mathrm{Fil}}^{\intercal} & 1 \end{pmatrix}. \tag{14}$$

Then, Nekovář's local height at p defined by (13) translates in our notation to the simple expression

$$h_p(M) = \chi_p\left(\gamma_\phi - \gamma_{\mathrm{Fil}} - \boldsymbol{\beta}_\phi^{\intercal}\cdot s_1(\boldsymbol{\alpha}_\phi) - \boldsymbol{\beta}_{\mathrm{Fil}}^{\intercal}\cdot s_2(\boldsymbol{\alpha}_\phi)\right). \tag{15}$$

3.4. **Twisting and p-adic heights.** We now use Nekovář's theory of p-adic heights to construct a quadratic Chabauty pair (θ, Υ). See [BD16, Section 5] for more details on the twisting construction.

Let $\mathbf{Z}_p[\![\pi_1^{\text{ét},p}(\overline{X},b)]\!] := \varprojlim \mathbf{Z}_p[\pi_1^{\text{ét}}(\overline{X},b)]/N$ where the limit is over all finite quotients of p-power order. Let I denote the augmentation ideal of $\mathbf{Q}_p\otimes_{\mathbf{Z}_p}\mathbf{Z}_p[\![\pi_1^{\text{ét},p}(\overline{X},b)]\!]$. Define the nilpotent algebra

$$A_n^{\text{ét}}(b) := \mathbf{Q}_p\otimes_{\mathbf{Z}_p}\mathbf{Z}_p[\![\pi_1^{\text{ét},p}(\overline{X},b)]\!]/I^{n+1}.$$

Then the limit of the A_n is isomorphic to the pro-universal enveloping algebra of the $\mathbf{Q}_p$-unipotent étale fundamental group of $\overline{X}$ at b (see [CK10]). There is an isomorphism

$$I^2/I^3 \simeq \mathrm{Coker}\left(\mathbf{Q}_p(1) \xrightarrow{\cup^*} V^{\otimes 2}\right).$$

Fix a nice correspondence $Z \in \mathrm{Pic}(X\times X)$ (or, more generally, in $\mathrm{Pic}(X\times X)\otimes\mathbf{Q}_p$, see Remark 2.5), and let U_Z denote the corresponding quotient of $\mathrm{U}_2^{\text{ét}}$ as defined in §2.3. We define the mixed extension $A_Z(b)$ to be the pushout of $A_2^{\text{ét}}(b)$ by

$$\mathrm{cl}_Z^* : \mathrm{Coker}\left(\mathbf{Q}_p(1)\xrightarrow{\cup^*} V^{\otimes 2}\right) \longrightarrow \mathbf{Q}_p(1),$$

see also [BD16, §5]. Then $A_Z(b)$ defines an element in $\mathcal{M}_{\mathrm{f}}(G_T;\mathbf{Q}_p,V,\mathbf{Q}_p(1))$, with respect to the I-adic filtration. The mixed extension $A_Z(b)$ is naturally equipped with a faithful Galois-equivariant action of U_Z which acts unipotently with respect to the filtration.

We use the twisting construction, see [Ser02, §5.3], to define $A_Z(b,x)$. Consider the maps

$$\begin{array}{rccccc} \tau & : & \mathrm{H}^1_{\mathrm{f}}(G_T,\mathrm{U}_Z) & \longrightarrow & \mathrm{M}_{\mathrm{f}}(G_T;\mathbf{Q}_p,V,\mathbf{Q}_p(1)), & P \longmapsto P\times_{\mathrm{U}_Z}A_Z(b),\\ \tau_p & : & \mathrm{H}^1_{\mathrm{f}}(G_p,\mathrm{U}_Z) & \longrightarrow & \mathrm{M}_{\mathrm{f}}(G_p;\mathbf{Q}_p,V,\mathbf{Q}_p(1)), & P \longmapsto P\times_{\mathrm{U}_Z}A_Z(b). \end{array}$$

As explained in [BD16, §5.1], τ is injective. When $x\in X(\mathbf{Q})$ and $P=\pi_1^{\text{ét}}(\overline{X};b,x)$, we denote

$$A_Z(b,x) := \tau([P]) = P\times_{\mathrm{U}_Z}A_Z(b).$$

If $x\in X(\mathbf{Q}_p)$ we likewise define $A_Z(b,x):=\tau_p([P])$ to be the mixed extension of G_p-modules obtained by twisting $A_Z(b)$. Similarly, we define $A_1(b,x)$ and $IA_Z(b,x)$ by twisting $A_1^{\text{ét}}(b)$ and $IA_Z(b)$.

We can now define (θ,Υ). Composing the twisting map with the unipotent Kummer map, we define

$$\theta \;:\; X(\mathbf{Q}_p) \longrightarrow \mathbf{Q}_p \;;\; x \longmapsto h_p\left(A_Z(b,x)\right). \tag{16}$$

Then, using the local heights h_v, for $v\in T_0$, we define the set

$$\Upsilon := \left\{\sum_{v\in T_0} h_v(A_Z(b,x_v)) : (x_v)\in\prod_{v\in T_0}X(\mathbf{Q}_v)\right\}\subset\mathbf{Q}_p. \tag{17}$$

It follows from Kim–Tamagawa [KT08, Corollary 0.2] that Υ is finite:

Theorem 3.5 (Kim–Tamagawa)**.** *If $v\neq p$, then $j_{2,v}^{\text{ét}}: X(\mathbf{Q}_v)\longrightarrow \mathrm{H}^1(G_v,\mathrm{U}_2)$ has finite image.*

We now prove that (θ,Υ) is a quadratic Chabauty pair, under the assumptions of §1.4.

Lemma 3.6. *Let X be as in §1.4. Then (θ,Υ) is a quadratic Chabauty pair. The endomorphism E is that induced by Z, the constant c is $[IA_Z(b)]$, and the bilinear pairing B is the global height h.*

Proof. By assumption, we have $r = g$ and $\mathrm{H}^1_{\mathrm{f}}(G_T, V) \simeq \mathrm{H}^1_{\mathrm{f}}(G_p, V) \simeq \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^*$, so we can indeed view the global height h as a bilinear pairing

$$h : \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^* \times \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^* \longrightarrow \mathbf{Q}_p\,.$$

We now check the conditions for a quadratic Chabauty pair. By [BD17, Lemma 10], the map

$$(\pi_*,\ h_p \circ \tau_p)\ :\ \mathrm{H}^1_{\mathrm{f}}(G_p, \mathrm{U}_Z)\ \longrightarrow\ \mathrm{H}^1_{\mathrm{f}}(G_p, V) \times \mathbf{Q}_p$$

is an isomorphism of schemes. Recall that $j^{\text{ét}}_{\mathrm{U}_Z, p}$ has Zariski dense image, so that the function

$$(\mathrm{AJ}_{\mathrm{b}}, \theta) = (\pi_*, h_p \circ \tau_p) \circ j^{\text{ét}}_{\mathrm{U}_Z, p},$$

which is defined by convergent power series on residue disks, also has Zariski dense image. As explained in [BD16, §5.2], we have for each $x \in X(\mathbf{Q})$ that

$$(\pi_1, \pi_2)(A_Z(b, x)) = (\mathrm{AJ}_{\mathrm{b}}(x), E(\mathrm{AJ}_{\mathrm{b}}(x)) + c).$$

where E is the endomorphism induced by Z, and $c = [IA_Z(b)]$. It follows from the decomposition $h = \sum_v h_v$ that when $B = h$ and $x \in X(\mathbf{Q})$, we have

$$\theta(x) - B(\mathrm{AJ}_{\mathrm{b}}(x), E(\mathrm{AJ}_{\mathrm{b}}(x)) + c) \in \Upsilon.$$ □

By Lemma 3.2 the local heights away from p are all trivial if X has potentially good reduction everywhere, so that $\Upsilon = \{0\}$. This is the case for $X = X_{\mathrm{s}}(13)$. We obtain:

Corollary 3.7. *If X has potential good reduction everywhere and satisfies the assumptions of §1.4, then $(\theta, \{0\})$ is a quadratic Chabauty pair, where $\theta = h_p(A_Z(b, .))$. The endomorphism E is that induced by Z, the constant c is $[IA_Z(b)]$, and the bilinear pairing B is the global height h.*

Remark 3.8. We say the splitting s of the Hodge filtration is *K-equivariant* if it commutes with the action of $K = \mathrm{End}(J) \otimes \mathbf{Q}$. If s is a K-equivariant splitting, then by [BD17, §4.1] the associated height pairing on any two extensions E_1, E_2 is K-equivariant, in the sense that for all $\alpha \in K$ we have

$$h(\alpha E_1, E_2) = h(E_1, \alpha E_2)$$

This decreases the number of rational points required to determine $X(\mathbf{Q})$ using quadratic Chabauty.

Remark 3.9. The character χ describes how to combine the various local classes in $\mathrm{H}^1(G_v, \mathbf{Q}_p(1))$. However, for a curve with potentially good reduction everywhere, the local heights away from p are trivial by Lemma 3.2, so the role of χ is reduced to providing an isomorphism of $\mathbf{Q}_p$-vector spaces

$$\mathbf{D}_{\mathrm{dR}}(\mathbf{Q}_p(1)) \simeq \mathrm{H}^1_{\mathrm{f}}(G_p, \mathbf{Q}_p(1)) \simeq \mathbf{Q}_p\,.$$

Remark 3.10. The extension class $[IA_Z(b)]$ is the p-adic realisation of the *Chow-Heegner* point associated to the Néron-Severi class Z (see e.g. [DRS12, Theorem 1]). As explained in Remark 5.5, the methods of this paper give an alternative approach to [DDLR15] for computing Chow–Heegner points, see equation (33).

4. Explicit computation of the p-adic height I: Hodge filtration

To complete the recipe for finding explicit finite sets containing $X(\mathbf{Q})$, it remains to choose a nice class $Z \in \mathrm{Pic}(X \times X) \otimes \mathbf{Q}_p$, and write the resulting locally analytic function

$$\theta\ :\ X(\mathbf{Q}_p)\ \longrightarrow\ \mathbf{Q}_p\ ;\ x\ \longmapsto\ h_p\left(A_Z(b, x)\right)$$

as a power series on every residue disk of $X(\mathbf{Q}_p)$. By equation (15), all that is needed is a sufficiently explicit description of the filtered ϕ-module $\mathbf{D}_{\mathrm{cris}}(A_Z(b, x))$. We compute the filtration and Frobenius separately, as pull-backs of certain universal objects $\mathcal{A}^{\mathrm{dR}}_Z$ and $\mathcal{A}^{\mathrm{rig}}_Z$ respectively. The filtration of $\mathcal{A}^{\mathrm{dR}}_Z$ is made explicit in this section following [BD17, §6], and the Frobenius structure is determined in §5.

4.1. **Notation.** Henceforth, X is a smooth projective curve of genus $g > 1$ over $\mathbf{Q}$, and $Y \subset X$ is an affine open subset. Let b be a rational point of Y which is integral at p. Suppose

$$\#(X \backslash Y)(\overline{\mathbf{Q}}) = d,$$

and let $K/\mathbf{Q}$ be a finite extension over which all the points of $D = X \backslash Y$ are defined. Choose a set $\omega_0, \ldots, \omega_{2g+d-2} \in \mathrm{H}^0(Y, \Omega^1)$ of differentials on Y, satisfying the following properties:

- The differentials $\omega_0, \ldots, \omega_{2g-1}$ are of the second kind on X, and form a *symplectic basis* of $\mathrm{H}^1_{\mathrm{dR}}(X)$, i.e. the cup product is the standard symplectic form with respect to this basis.
- The differentials $\omega_{2g}, \ldots, \omega_{2g+d-2}$ are of the third kind on X, i.e. a differential all of whose poles have order one.

We set $V_{\mathrm{dR}}(Y) := \mathrm{H}^1_{\mathrm{dR}}(Y)^*$, and let $T_0, \ldots, T_{2g+d-2}$ be the dual basis.

4.2. **The universal filtered connection $\mathcal{A}_n^{\mathrm{dR}}$.** Let $\mathcal{C}^{\mathrm{dR}}(X_K)$ the category of unipotent vector bundles with connection on X_K. Our base point $b \in X(K)$ makes $\mathcal{C}^{\mathrm{dR}}(X_K)$ into a unipotent Tannakian category, whose fundamental group we denote by $\pi_1^{\mathrm{dR}}(X, b)$. Using the notation from the appendix, we define

$$A_n^{\mathrm{dR}}(b) = A_n(\mathcal{C}^{\mathrm{dR}}(X_K, b^*)),$$

with associated path torsors $A_n^{\mathrm{dR}}(b, x)$. Let $\mathcal{A}_n^{\mathrm{dR}}(b)$, or simply $\mathcal{A}_n^{\mathrm{dR}}$, be the universal n-unipotent object, associated to the $\pi_1^{\mathrm{dR}}(X, b)$-representation $A_n^{\mathrm{dR}}(b)$ via the Tannaka equivalence, see § A.1.2. This vector bundle carries a Hodge filtration, with the property that the K-vector space isomorphism

$$x^* \mathcal{A}_n^{\mathrm{dR}}(b) \simeq A_n^{\mathrm{dR}}(b, x), \qquad \forall x : \mathrm{Spec}(K) \longrightarrow X_K$$

is an isomorphism of filtered vector spaces. For more details, see also [Kim09, pp. 98–100].

We now describe a closely related bundle $\mathcal{A}_n^{\mathrm{dR}}(Y)$ on the affine open Y, using the notation from §4.1. This bundle admits a very simple description, and its relation with $\mathcal{A}_n^{\mathrm{dR}}$ is given in Corollary 4.3. To distinguish it more clearly from $\mathcal{A}_n^{\mathrm{dR}}(Y)$, we will denote $\mathcal{A}_n^{\mathrm{dR}}$ by $\mathcal{A}_n^{\mathrm{dR}}(X)$ in this paragraph.

Set $\mathcal{A}_n^{\mathrm{dR}}(Y) := \bigoplus_{i=0}^n V_{\mathrm{dR}}(Y)^{\otimes i} \otimes \mathcal{O}_Y$, and define the connection

$$\nabla_n \ : \ \mathcal{A}_n^{\mathrm{dR}}(Y) \longrightarrow \mathcal{A}_n^{\mathrm{dR}}(Y) \otimes \Omega^1_Y \ , \qquad \nabla_n(v \otimes 1) \ = \ \sum_{i=0}^{2g+d-2} -(T_i \otimes v) \otimes \omega_i, \tag{18}$$

Then $\mathcal{A}_n^{\mathrm{dR}}(Y)$ is n-step unipotent, in the sense that it has a filtration

$$\bigoplus_{i=j}^{n} V_{\mathrm{dR}}(Y)^{\otimes i} \otimes \mathcal{O}_Y, \qquad \text{for } j = 0, 1, \ldots, n$$

by subbundles preserved by ∇, where the graded pieces inherit the trivial connection. The following theorem, proved by Kim [Kim09], provides a universal property for the bundle $\mathcal{A}_n^{\mathrm{dR}}(Y)$.

Theorem 4.1 (Kim)**.** *Let $\mathbf{1} = 1 \otimes 1$ be the identity section of $\mathcal{A}_n^{\mathrm{dR}}(Y)$. Then $(\mathcal{A}_n^{\mathrm{dR}}(Y), \mathbf{1})$ is a n-step universal pointed object, in the sense of §A.1. That is, for any n-step unipotent vector bundle $\mathcal{V}$ with connection on Y, and any section v of $\mathcal{V}$, there exists a unique map*

$$f : \mathcal{A}_n^{\mathrm{dR}}(Y) \longrightarrow \mathcal{V} \qquad \text{such that} \quad f(\mathbf{1}) = v.$$

Although universal properties mean $(\mathcal{A}_n^{\mathrm{dR}}(Y), \mathbf{1})$ is unique up to unique isomorphism, the trivialisation of the underlying vector bundle above is not unique, as it depends on a choice of elements of $\mathrm{H}^0(Y, \Omega^1)$ defining a basis of $\mathrm{H}^1_{\mathrm{dR}}(Y)$. The trivialisation has some relation to the algebraic structure of the spaces $A_n^{\mathrm{dR}}(b, x)$, which we now explain. For $x \in Y(K)$, it gives is a canonical isomorphism

$$s_0(b, x) : \bigoplus_{i=0}^{n} V_{\mathrm{dR}}(Y)^{\otimes i} \longrightarrow \ A_n^{\mathrm{dR}}(Y)(b, x) := x^* \mathcal{A}_n^{\mathrm{dR}}(Y).$$

The left hand side has a natural algebra structure, by viewing it as a quotient of the tensor algebra of $V_{\mathrm{dR}}(Y)$. On the other hand, for all $x_1, x_2, x_3 \in Y(K)$ we have (see Appendix §A.1) maps

$$A_n^{\mathrm{dR}}(Y)(x_2, x_3) \times A_n^{\mathrm{dR}}(Y)(x_1, x_2) \longrightarrow A_n^{\mathrm{dR}}(Y)(x_1, x_3).$$

coming from the surjections $\mathrm{Hom}(x_i^*, x_j^*) \to A_n^{\mathrm{dR}}(Y)(x_i, x_j)$ and the composition of natural transformations

$$\mathrm{Hom}(x_2, x_3) \times \mathrm{Hom}(x_1, x_2) \longrightarrow \mathrm{Hom}(x_1, x_3).$$

Lemma 4.2. *For all $f_1, f_2 \in A_n^{\mathrm{dR}}(Y)$, and all $x_1, x_2, x_3 \in Y(K)$,*

$$s_0(x_1, x_3)(f_2 f_1) = s_0(x_2, x_3)(f_2) s_0(x_1, x_2)(f_1).$$

Proof. As in the appendix, let $\mathcal{C}^{\mathrm{dR}}(Y)_n$ denote the category of connections which are i-unipotent for $i \leq n$. Let x_{1n}, x_{2n}, x_{3n} denote the fibre functors corresponding to the points x_1, x_2, x_3. Let α_{x_i, x_j} denote the isomorphism $A_n^{\mathrm{dR}}(Y)(x_i, x_j) \simeq \mathrm{Hom}(x_{in}, x_{jn})$. Then $\alpha_{x_2,x_3}(s_0(x_2, x_3)(f_2)) \in \mathrm{Hom}(x_{2n}, x_{3n})$, and $s_0(x_1, x_2)(f_1) \in x_2^* \mathcal{A}_n^{\mathrm{dR}}(Y)$, and to prove the lemma it is enough to prove that

$$(\alpha_{x_2,x_3}(s_0(x_2, x_3)(f_2)))(s_0(x_1, x_2)(f_1)) = s_0(x_1, x_3)(f_2 f_1)$$

in $x_3^* \mathcal{A}_n^{\mathrm{dR}}(Y)$. To prove this, note that there is a morphism of connections $F_1 : \mathcal{A}_n^{\mathrm{dR}}(Y) \to \mathcal{A}_n^{\mathrm{dR}}(Y)$ given by sending v to $v f_1$. Hence the lemma follows from commutativity of

$$\begin{array}{ccc} x_2^* \mathcal{A}_n^{\mathrm{dR}}(Y) & \xrightarrow{\alpha} & x_3^* \mathcal{A}_n^{\mathrm{dR}}(Y) \\ \downarrow{\scriptstyle x_2^* F} & & \downarrow{\scriptstyle x_3^* F} \\ x_2^* \mathcal{A}_n^{\mathrm{dR}}(Y) & \xrightarrow{\alpha} & x_3^* \mathcal{A}_n^{\mathrm{dR}}(Y). \end{array}$$

where $\alpha := \alpha_{x_2,x_3}(s_0(x_2, x_3)(f_2))(\mathcal{A}_n^{\mathrm{dR}}(Y))$ □

The following result describes the relation between $\mathcal{A}_n^{\mathrm{dR}}(X)$ and $\mathcal{A}_n^{\mathrm{dR}}(Y)$, see also [BD17, Lemma 6.2].

Corollary 4.3. *The connection $\mathcal{A}_n^{\mathrm{dR}}(X)|_Y$ is the maximal quotient of $\mathcal{A}_n^{\mathrm{dR}}(Y)$ which extends to a holomorphic connection (i.e. without log singularities) on the whole of X.*

Proof. It is enough to show that, for any surjection of left $\pi_1^{\mathrm{dR}}(Y, b)$-modules

$$p : A_n^{\mathrm{dR}}(Y) \longrightarrow N,$$

the associated connection $\mathcal{N}$ extends to a connection on X without log singularities if and only if p factors through the surjection $A_n^{\mathrm{dR}}(Y) \longrightarrow A_n^{\mathrm{dR}}(X)$. The latter occurs if and only if N is the pullback of a left $\pi_1^{\mathrm{dR}}(X, b)$-module. The corollary follows by the Tannaka equivalence between left $\pi_1^{\mathrm{dR}}(X, b)$-modules, and unipotent connections on X. □

4.3. **The Hodge filtration on $\mathcal{A}_n^{\mathrm{dR}}$.** In what follows, we will need to explicitly compute the Hodge filtration of $\mathcal{A}_2^{\mathrm{dR}}$, or rather of a certain quotient $\mathcal{A}_Z$. To this end, we now state a characterisation of this Hodge filtration via a universal property, due to Hadian [Had11].

Recall that a *filtered connection* is defined to be a connection $(\mathcal{V}, \nabla)$ on X, together with an exhaustive descending filtration

$$\ldots \supset \mathrm{Fil}^i \mathcal{V} \supset \mathrm{Fil}^{i+1} \mathcal{V} \supset \ldots$$

satisfying the Griffiths transversality property

$$\nabla(\mathrm{Fil}^i \mathcal{V}) \subset (\mathrm{Fil}^{i-1} \mathcal{V}) \otimes \Omega^1.$$

A morphism of filtered connections is one that preserves the filtrations and commutes with ∇.

The universal n-unipotent bundle $\mathcal{A}_n^{\mathrm{dR}}(b)$ is associated to the $\pi_1^{\mathrm{dR}}(X,b)$-representation $A_n^{\mathrm{dR}}(b)$, and there is a natural exact sequence of representations

$$0 \longrightarrow I^n/I^{n+1} \longrightarrow A_n^{\mathrm{dR}}(b) \longrightarrow A_{n-1}^{\mathrm{dR}}(b) \longrightarrow 0$$

where the kernel I^n/I^{n+1} has trivial $\pi_1^{\mathrm{dR}}(X,b)$-action. This means that the kernel

$$\mathcal{A}^{\mathrm{dR}}[n] \;:=\; \mathrm{Ker}\left(\mathcal{A}_n^{\mathrm{dR}}(b) \longrightarrow \mathcal{A}_{n-1}^{\mathrm{dR}}(b)\right) \;\simeq\; I^n/I^{n+1} \otimes \mathcal{O}_X,$$

is a trivial bundle with connection. The natural surjection $(I/I^2)^{\otimes n} \longrightarrow I^n/I^{n+1}$ gives rise to a surjection $V_{\mathrm{dR}}^{\otimes n} \otimes \mathcal{O}_X \longrightarrow \mathcal{A}^{\mathrm{dR}}[n]$. The Hodge filtration on V_{dR} gives $\mathcal{A}^{\mathrm{dR}}[n]$ its structure of a filtered connection. As explained in [BD17], the Hodge filtration on $\mathcal{A}_n^{\mathrm{dR}}(b)$ may now be characterised using Hadian's universal property, proved in [Had11].

Theorem 4.4 (Hadian)**.** *For all $n > 0$, the Hodge filtration $\mathrm{Fil}^\bullet$ on $\mathcal{A}_n^{\mathrm{dR}}(b)$ is the unique filtration such that*

- $\mathrm{Fil}^\bullet$ *makes $(\mathcal{A}_n^{\mathrm{dR}}(b), \nabla)$ into a filtered connection,*
- *The natural maps induce a sequence of filtered connections:*
$$V_{\mathrm{dR}}^{\otimes n} \otimes \mathcal{O}_X \longrightarrow \mathcal{A}_n^{\mathrm{dR}}(b) \longrightarrow \mathcal{A}_{n-1}^{\mathrm{dR}}(b) \longrightarrow 0,$$
- *The identity element of $A_n^{\mathrm{dR}}(b)$ lies in $\mathrm{Fil}^0 A_n^{\mathrm{dR}}(b)$.*

4.4. **The filtered connection $\mathcal{A}_Z$.** As in §3, a central role is played by a Tate class, which will come from an algebraic cycle on $X \times X$. Since the contribution to the p-adic height is entirely through its realisation as a p-adic de Rham class, we phrase things in this language. Henceforth, let

$$Z = \sum Z_{ij}\omega_i \otimes \omega_j \in \mathrm{H}^1_{\mathrm{dR}}(X) \otimes \mathrm{H}^1_{\mathrm{dR}}(X)$$

be a nonzero cohomology class satisfying the following conditions:

(a) Z is in $(\mathrm{H}^1_{\mathrm{dR}}(X) \otimes \mathrm{H}^1_{\mathrm{dR}}(X))^{\phi=p}$.
(b) Z is in $\mathrm{Fil}^1(\mathrm{H}^1_{\mathrm{dR}}(X) \otimes \mathrm{H}^1_{\mathrm{dR}}(X))$.
(c) Z maps to zero under the cup product
$$\cup \;:\; \mathrm{H}^1_{\mathrm{dR}}(X) \otimes \mathrm{H}^1_{\mathrm{dR}}(X) \longrightarrow \mathrm{H}^2_{\mathrm{dR}}(X).$$
(d) Z maps to zero under the symmetrisation map
$$\mathrm{H}^1_{\mathrm{dR}}(X) \otimes \mathrm{H}^1_{\mathrm{dR}}(X) \longrightarrow \mathrm{Sym}^2 \mathrm{H}^1_{\mathrm{dR}}(X).$$

By property (d), we may henceforth think of Z as an element of $\mathrm{H}^2_{\mathrm{dR}}(\mathrm{J}_{\mathbf{Q}_p})$. It follows from Lemma 2.4 that the Tate class associated to a nice correspondence satisfies these properties. Though we will not need it in the sequel, the following result gives a converse to this statement.

Lemma 4.5. *Let Z be a class satisfying properties (a)–(d). If $\rho(\mathrm{J}) = \rho(\mathrm{J}_{\mathbf{Q}_p})$, then there exists a nice element of $\mathrm{Pic}(X \times X) \otimes \mathbf{Q}_p$ mapping to Z.*

Proof. By the Tate conjecture for H^2 of abelian varieties over finite fields, property (a) of Z guarantees that it comes from a $\mathbf{Q}_p$-divisor on $\mathrm{J}_{\mathbf{F}_p}$. By the p-adic Lefschetz (1,1)-theorem of Berthelot–Ogus [BO83, §3.8], property (b) implies that it lifts to something in $\mathrm{NS}(\mathrm{J}_{\mathbf{Q}_p}) \otimes \mathbf{Q}_p$. By hypothesis, the map $\mathrm{NS}(\mathrm{J}_{\mathbf{Q}}) \otimes \mathbf{Q}_p \to \mathrm{NS}(\mathrm{J}_{\mathbf{Q}_p}) \otimes \mathbf{Q}_p$ is an isomorphism, hence Z comes from a $\mathbf{Q}_p$-divisor on $\mathrm{J}_{\mathbf{Q}}$. Finally, the element of $\mathrm{Pic}(X \times X) \otimes \mathbf{Q}_p$ corresponding to this cycle is nice by property (c) of Z. □

We now come to the definition of the main object of this section and the next. Recall that we have an exact sequence of filtered connections

$$0 \longrightarrow \mathcal{A}^{\mathrm{dR}}[2] \longrightarrow \mathcal{A}_2^{\mathrm{dR}} \longrightarrow \mathcal{A}_1^{\mathrm{dR}} \longrightarrow 0, \tag{19}$$

and an isomorphism of filtered vector spaces

$$\mathcal{A}^{\mathrm{dR}}[2] \simeq \mathrm{Coker}\left(\mathbf{Q}_p(1) \xrightarrow{\cup^*} V_{\mathrm{dR}}^{\otimes 2}\right) \otimes \mathcal{O}_X.$$

Define $\mathcal{A}_Z(b)$, or simply $\mathcal{A}_Z$, to be the quotient of $\mathcal{A}_2^{\mathrm{dR}}$ obtained by pushing out (19) along

$$Z \ : \ V_{\mathrm{dR}} \otimes V_{\mathrm{dR}} \longrightarrow \mathbf{Q}_p(1),$$

which by property (c) of Z factors through $V_{\mathrm{dR}}^{\otimes 2}/\mathrm{Im}\cup^*$. The importance of this definition lies in the fact that, as we will see in §5, we can endow $\mathcal{A}_Z$ with a Frobenius structure such that we have an isomorphism of filtered ϕ-modules

$$x^*\,\mathcal{A}_Z \simeq \mathbf{D}_{\mathrm{cris}}(A_Z(b,x)).$$

The Frobenius structure on $\mathcal{A}_Z$ is the subject of §5, and in the remainder of this section we will explicitly compute the connection and Hodge filtration on $\mathcal{A}_Z$.

Using the results of §4.2, we may describe the connection of $\mathcal{A}_Z$ explicitly on the affine open Y. We use the notation of §4.1, and denote the matrix of the correspondence Z on $\mathrm{H}^1_{\mathrm{dR}}(X)$ also by Z, where we act on column vectors. Then via Theorem 4.1, we obtain a trivialisation

$$s_0(b,.) : \mathcal{O}_Y \otimes \left(\mathbf{Q}_p \oplus V_{\mathrm{dR}} \oplus \mathbf{Q}_p(1)\right) \xrightarrow{\sim} \mathcal{A}_Z(b)|_Y.$$

When there is no risk of confusion we will occasionally write this simply as s_0. By Corollary 4.3 and the explicit description of the connection on $\mathcal{A}_n^{\mathrm{dR}}(Y)$ given in (18), we have that the connection ∇ on $\mathcal{A}_Z$ via the trivialisation s_0 is given by

$$s_0^{-1} \circ \nabla \circ s_0 = d + \Lambda, \qquad \text{where} \quad \Lambda := -\begin{pmatrix} 0 & 0 & 0 \\ \boldsymbol{\omega} & 0 & 0 \\ \eta & \boldsymbol{\omega}^{\intercal} Z & 0 \end{pmatrix}, \tag{20}$$

for some differential η of the third kind on X. This differential is uniquely determined by the conditions that it is in the space spanned by $\omega_{2g}, \ldots, \omega_{2g+d-2}$, and that the connection ∇ extends to a holomorphic connection on the whole of X, as in Corollary 4.3.

Remark 4.6. In the notation above, and henceforth in this paper, block matrices are taken with respect to the 2-step unipotent filtration with basis $\mathbf{1}, T_0, \ldots, T_{2g-1}, S$, and we use the notation $\boldsymbol{\omega}$ for the column vector with entries $\omega_0, \ldots, \omega_{2g-1}$.

4.5. **The Hodge filtration of $\mathcal{A}_Z$.** We now make the Hodge filtration on $\mathcal{A}_Z$ explicit. We will use Theorem 4.4, and our knowledge of the Hodge filtration on the first quotient $\mathcal{A}_1$, to uniquely determine the Hodge filtration on $\mathcal{A}_Z$ using the exact sequence of filtered connections

$$0 \longrightarrow \mathbf{Q}_p(1) \otimes \mathcal{O}_X \longrightarrow \mathcal{A}_Z \longrightarrow \mathcal{A}_1 \longrightarrow 0.$$

It is easy to see that $s_0(\mathrm{Fil}^0 V_{\mathrm{dR}} \oplus \mathbf{Q}_p)$ extends to a sub-bundle of $\mathcal{A}_1$, hence Hadian's theorem implies that this sub-bundle is $\mathrm{Fil}^0 \mathcal{A}_1$. To lift this to a sub-bundle of $\mathcal{A}_Z$, recall the explicit description of the connection ∇ on the restriction of $\mathcal{A}_Z$ to Y, given by (20) with respect to the basis $\mathbf{1}, T_0, \ldots, T_{2g-1}, S$. In analogy with the notation of §3.3, we may specify the Hodge filtration by giving an isomorphism of filtered vector bundles

$$s^{\mathrm{Fil}} \ : \ \left(\mathbf{Q}_p \oplus V_{\mathrm{dR}} \oplus \mathbf{Q}_p(1)\right) \otimes \mathcal{O}_Y \xrightarrow{\sim} \mathcal{A}_Z\,|_Y,$$

where the filtration on the left hand side is induced from the Hodge filtration on its graded pieces. Such a morphism s^{Fil} is uniquely determined by the vector $\boldsymbol{\beta}_{\mathrm{Fil}}$ and $\gamma_{\mathrm{Fil}} \in \mathrm{H}^0(Y, \mathcal{O}_Y)$ in

$$s_0^{-1} \circ s^{\mathrm{Fil}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \gamma_{\mathrm{Fil}} & \boldsymbol{\beta}_{\mathrm{Fil}}^{\intercal} & 1 \end{pmatrix}.$$

The conditions imposed by Theorem 4.4 determine γ_{Fil} and $\boldsymbol{\beta}_{\mathrm{Fil}}$ uniquely, as we will now explain. At each point x in $D = X - Y$, defined over K, let

$$s_x \ : \ \Big((\mathbf{Q}_p \oplus V_{\mathrm{dR}} \oplus \mathbf{Q}_p(1)) \otimes K[\![t_x]\!],\ d \Big) \xrightarrow{\sim} \big(\mathcal{A}_Z\,|_{K[\![t_x]\!]},\ \nabla \big)$$

be a trivialisation of $\mathcal{A}_Z$ in a formal neighbourhood of x, with local parameter t_x. The difference between the bundle trivialisations defines a gauge transformation

$$C_x := s_x^{-1} \circ s_0 \ \in \ \mathrm{End}\big(\mathbf{Q}_p \oplus V_{\mathrm{dR}} \oplus \mathbf{Q}_p(1) \big) \otimes K(\!(t_x)\!)$$

satisfying

$$C_x^{-1} dC_x = \Lambda. \tag{21}$$

Conversely, any such C_x defines a trivialisation s_x. Expanding out (21) shows that C_x is of the form

$$C_x = \begin{pmatrix} 1 & 0 & 0 \\ \boldsymbol{\Omega}_x & 1 & 0 \\ g_x & \boldsymbol{\Omega}_x^{\intercal} Z & 1 \end{pmatrix}, \quad \text{where} \ \begin{cases} d\boldsymbol{\Omega}_x &= -\boldsymbol{\omega} \\ dg_x &= \boldsymbol{\Omega}_x^{\intercal} Z d\boldsymbol{\Omega}_x - \eta. \end{cases} \tag{22}$$

Equivalently, the gauge transformation C_x defines a basis of formal horizontal sections of $\mathcal{A}_Z$ at x. By Theorem 4.4, $\mathrm{Fil}^0 \mathcal{A}_Z\,|_Y$ extends to a bundle on X, which results in the condition that the functions in $\boldsymbol{\beta}_{\mathrm{Fil}}$ extend to holomorphic functions on X, and are hence constant, as well as the condition

$$g_x + \gamma_{\mathrm{Fil}} - \boldsymbol{\beta}_{\mathrm{Fil}}^{\intercal} \cdot \boldsymbol{\Omega}_x - \boldsymbol{\Omega}_x^{\intercal} Z s_2(\boldsymbol{\Omega}_x) \quad \in \quad K[\![t_x]\!],$$

see also [BD17, §6.4]. The existence and uniqueness follow from the following lemma, which follows from Riemann–Roch. We omit the proof, see [BD17, Lemma 25] for a similar argument.

Lemma 4.7. *Given any tuple $(g_x) \in \prod_{x \in D} K(\!(t_x)\!)$, there exists a unique vector of constants $\boldsymbol{\beta} \in K^{2g}$ and a function $\gamma \in \mathrm{H}^0(Y, \mathcal{O})$, unique modulo constants, such that for all $x \in D$,*

$$g_x + \gamma - \boldsymbol{\beta}^{\intercal} \cdot \boldsymbol{\Omega}_x - \boldsymbol{\Omega}_x^{\intercal} Z s_2(\boldsymbol{\Omega}_x) \quad \in \quad K[\![t_x]\!],$$

By the above lemma, we can determine the vector of constants $\boldsymbol{\beta}_{\mathrm{Fil}}$ uniquely, and γ_{Fil} is uniquely determined by the additional condition that $\gamma_{\mathrm{Fil}}(b) = 0$. In summary, this gives the following algorithm for computing the Hodge filtration on $\mathcal{A}_Z^{\mathrm{dR}}$.

(i) Compute η as in (20), as the unique linear combination of $\omega_{2g}, \ldots, \omega_{2g+d-2}$ such that

$$d\boldsymbol{\Omega}_x^{\intercal} Z \boldsymbol{\Omega}_x - \eta$$

has vanishing residue at all $x \in X \backslash Y$.

(ii) For all $x \in X \backslash Y$, compute power series for $\boldsymbol{\omega}_x$ and η up to large enough precision, which means at least $\pmod{t_x^{d_x}}$, where d_x is the order of the largest pole occurring. Use this to solve the system of equations (22) for g_x in $K(\!(t_x)\!)/K[\![t_x]\!]$.

(iii) Compute the constants $\boldsymbol{\beta}_{\mathrm{Fil}}$ and function γ_{Fil} characterised by $\gamma_{\mathrm{Fil}}(b) = 0$ and

$$g_x + \gamma_{\mathrm{Fil}} - \boldsymbol{\beta}_{\mathrm{Fil}}^{\intercal} \cdot \boldsymbol{\Omega}_x - \boldsymbol{\Omega}_x^{\intercal} Z s_2(\boldsymbol{\Omega}_x) \quad \in \quad K[\![t_x]\!].$$

5. Explicit computation of the p-adic height II: Frobenius

The preceding section gives a computationally feasible method for computing the Hodge filtration on the module $\mathbf{D}_{\mathrm{cris}}(A_Z(b, x))$. We now describe its Frobenius structure. When X is hyperelliptic, such a description was given in [BD17, §6]. We give a description in general, in terms of the Frobenius structure on the isocrystal $\mathcal{A}_Z^{\mathrm{rig}}(\bar{b})$, and compute the latter using universal properties.

5.1. **The Frobenius structure on $\mathcal{A}_n^{\mathrm{rig}}$.** We first describe the Frobenius structure on the universal n-step unipotent connection $\mathcal{A}_n^{\mathrm{dR}}(b)$. We henceforth assume that $\mathcal{X}\backslash\mathcal{Y}$ is smooth over $\mathbf{Z}_p$. Some background on unipotent isocrystals can be found in §A.2, and we adopt the notation used there.

Let $\mathcal{C}^{\mathrm{rig}}(\mathcal{X}_{\mathbf{F}_p})$ be the category of unipotent isocrystals on the special fibre of $\mathcal{X}$. Pull-back by absolute Frobenius induces an auto-equivalence of $\mathcal{C}^{\mathrm{rig}}(\mathcal{X}_{\mathbf{F}_p})$ [CS99, Proposition 2.4.2], which yields an action on the path torsors $\pi_1^{\mathrm{rig}}(\mathcal{X}_{\mathbf{F}_p};\overline{b},\overline{x})$ of its fundamental group, and hence on the n-step unipotent quotients:

$$\phi_n : A_n^{\mathrm{rig}}(\overline{b},\overline{x}) \longrightarrow A_n^{\mathrm{rig}}(\overline{b},\overline{x}).$$

On the other hand, pull-back by absolute Frobenius on $\mathcal{C}^{\mathrm{rig}}(\mathcal{X}_{\mathbf{F}_p})$ induces an auto-equivalence. Therefore, if $(\mathcal{A}_n^{\mathrm{rig}}(\overline{b}),1)$ is the universal n-step unipotent pointed object, so is its pullback, and hence they are canonically isomorphic, yielding a Frobenius structure on $\mathcal{A}_n^{\mathrm{rig}}(\overline{b})$. To describe this Frobenius structure explicitly on the realisation given by the rigid triple $(Y,X,\mathfrak{X})$, let $\mathcal{U}\subset\mathcal{Y}$ be a Zariski open subset, and let $\mathfrak{X},\mathfrak{U}$ denote the formal completions of $\mathcal{X}$ and $\mathcal{U}$ along their special fibres. Choose a lift of Frobenius

$$\phi : \mathfrak{U} \longrightarrow \mathfrak{U}$$

which extends to a strict open neighbourhood of $]\mathcal{U}_{\mathbf{F}_p}[$. Then the Frobenius structure is an isomorphism

$$\Phi_n : \phi^*\mathcal{A}_n^{\mathrm{rig}}(\overline{b}) \xrightarrow{\sim} \mathcal{A}_n^{\mathrm{rig}}(\overline{b})$$

of overconvergent isocrystals on $(Y,X,\mathfrak{X})$. By the functoriality of the isomorphism in Lemma A.4, we obtain for all points $\overline{x}\in\mathcal{U}(\mathbf{F}_p)$ with Teichmüller representative x_0 a commutative diagram

$$\begin{array}{ccc} x_0^*\,\mathcal{A}_n^{\mathrm{rig}}(\overline{b}) & \xrightarrow{x_0^*\Phi_n} & x_0^*\,\mathcal{A}_n^{\mathrm{rig}}(\overline{b}) \\ \downarrow\wr & & \downarrow\wr \\ A_n^{\mathrm{rig}}(\overline{b},\overline{x}) & \xrightarrow{\phi_n} & A_n^{\mathrm{rig}}(\overline{b},\overline{x}) \end{array} \tag{23}$$

To compute ϕ_n on $A_n^{\mathrm{rig}}(\overline{b},\overline{x})$, we are reduced to describing the Frobenius structure Φ_n on the isocrystal $\mathcal{A}_n^{\mathrm{rig}}(\overline{b})$, which has the advantage of being characterised by the following universal property.

Lemma 5.1. *The Frobenius structure on $\mathcal{U}_{\mathbf{F}_p}$ for $\mathcal{A}_n^{\mathrm{rig}}(\overline{b})$ is the unique morphism*

$$\Phi_n : \phi^*\,\mathcal{A}_n^{\mathrm{rig}}(\overline{b}) \longrightarrow \mathcal{A}_n^{\mathrm{rig}}(\overline{b}) \tag{24}$$

which, in the fibre at $\overline{b}$, sends 1 to 1.

Proof. The Frobenius endomorphism in $\mathrm{Hom}(\overline{b}^*,\overline{b}^*)$ is a morphism of unital algebras, and hence the Frobenius structure satisfies this property. As explained in §A.1, a morphism of n-unipotent universal objects is determined by where it sends $1\in\overline{b}^*\,\mathcal{A}_n^{\mathrm{rig}}(\overline{b})$, which shows uniqueness. □

5.2. **The Frobenius operator on $A_n^{\mathrm{dR}}(b,x)$.** We now explain how to define Frobenius operators on $A_n^{\mathrm{dR}}(b,x)$. They will be computed explicitly in the next section on the quotient $A_Z^{\mathrm{dR}}(b,x)$. We start by recalling the following comparison theorem of Chiarellotto–Le Stum [CS99, Proposition 2.4.1].

Theorem 5.2 (Chiarellotto–Le Stum)**.** *The analytification functor defines an equivalence of categories*

$$(-)^{\mathrm{an}} \;:\; \mathcal{C}^{\mathrm{dR}}(X_{\mathbf{Q}_p}) \xrightarrow{\sim} \mathcal{C}^{\mathrm{rig}}(\mathcal{X}_{\mathbf{F}_p}),$$

and for any $x\in X(\mathbf{Q}_p)$ with reduction $\overline{x}$, we have a canonical isomorphism of fibre functors

$$\iota_x : \overline{x}^*\circ(-)^{\mathrm{an}} \simeq x^*,$$

such that if $x,y\in X(\mathbf{Q}_p)$ belong to the same residue disk, the canonical isomorphism $\iota_x\circ\iota_y^{-1}$ is given by parallel transport $T_{x,y}$ along the connection, as described in §A.2.

Via ι_b and ι_x, the pull-back of absolute Frobenius on $\mathcal{X}_{\mathbf{F}_p}$ gives a Frobenius action on the fundamental group $\pi_1^{\mathrm{dR}}(X_{\mathbf{Q}_p}; b, x)$, and therefore a Frobenius operator on the quotient

$$\phi_n(b,x) : A_n^{\mathrm{dR}}(b,x) \longrightarrow A_n^{\mathrm{dR}}(b,x).$$

This Frobenius operator may be related to the isocrystal $\mathcal{A}_n^{\mathrm{rig}}(\bar{b})$ as follows. Let b_0, x_0 be Teichmüller representatives of b, x. We then have the equality

$$\phi_n(b,x) = \tau_{b,x} \circ \phi_n(b_0,x_0) \circ \tau_{b,x}^{-1},$$

with $\tau_{b,x}$ the canonical isomorphism provided by Theorem 5.2, given by

$$\tau_{b,x} : \mathrm{Hom}(b_0^*, x_0^*) \xrightarrow{\sim} \mathrm{Hom}(b^*, x^*), \quad g \mapsto T_{x,x_0} \circ g \circ T_{b_0,b}$$

5.2.1. *Parallel transport.* We can describe the effect of $\tau_{b,x}$ on $A_n^{\mathrm{dR}}(b,x)$ explicitly via formal integration on residue disks. Since $A_n^{\mathrm{dR}}(b,x)$ is a quotient of $A_n^{\mathrm{dR}}(Y)(b,x)$, it suffices to describe parallel transport on the latter. Recall the trivialisation

$$s_0(b,x) \ : \ \bigoplus_{i=0}^{n} V_{\mathrm{dR}}(Y)^{\otimes i} \xrightarrow{\sim} A_n^{\mathrm{dR}}(Y)(b,x) \tag{25}$$

from Section §4.2. We showed in Lemma 4.2 that via this trivialisation, the composition of functors

$$\mathrm{Hom}(x_0^*, x^*) \times \mathrm{Hom}(b_0^*, x_0^*) \times \mathrm{Hom}(b^*, b_0^*) \longrightarrow \mathrm{Hom}(b^*, x^*)$$

acting on $\mathcal{A}_n^{\mathrm{dR}}(Y)$ corresponds to multiplication in the algebra. To explicitly describe parallel transport, define for any two $x_1, x_2 \in X(\mathbf{Q}_p)$ on the same residue disk

$$\mathbf{I}(x_1,x_2) = 1 + \sum_w \int_{x_1}^{x_2} w(\omega_0, \ldots, \omega_{2g+2d-2}) \qquad \text{in} \quad \bigoplus_{i=0}^{n} V_{\mathrm{dR}}(Y)^{\otimes i} \tag{26}$$

where the sum is over all words w in $\{T_0, \ldots, T_{2g+d-2}\}$ of length at most n, and where $w(\omega_0, \ldots, \omega_{2g+d-2})$ is defined to be the word in $\{\omega_0, \ldots, \omega_{2g+d-2}\}$ obtained by substituting ω_i for T_i. Here, the integrals are given by formal integration of power series on the residue disk of x_1 and x_2. Then $\tau_{b,x}$, when considered as an operator on $\mathcal{A}_n^{\mathrm{dR}}(Y)$ via the trivialisation (25), is given by the left-right multiplication map

$$\tau_{b,x} : \bigoplus_{i=0}^{n} V_{\mathrm{dR}}(Y)^{\otimes i} \xrightarrow{\sim} \bigoplus_{i=0}^{n} V_{\mathrm{dR}}(Y)^{\otimes i}, \quad v \mapsto \mathbf{I}(x_0,x) v \, \mathbf{I}(b,b_0). \tag{27}$$

By Besser's theory of Coleman integration on unipotent connections, we have that, for *any* $b, b_0, x, x_0 \in Y(\mathbf{Q}_p)$, the same formula (27) describes the unique unipotent Frobenius-equivariant isomorphism

$$A_n^{\mathrm{dR}}(b_0,x_0) \longrightarrow A_n^{\mathrm{dR}}(b,x)$$

if the integrals in (26) are instead interpreted in the sense of Coleman integration.

5.2.2. *Frobenius on $A_n^{\mathrm{dR}}(b_0,x_0)$.* The operator $\phi_n(b_0,x_0)$ is related to the isocrystal $\mathcal{A}_n^{\mathrm{rig}}(\bar{b})$ via

$$\begin{array}{ccc} x_0^* \mathcal{A}_n^{\mathrm{rig}}(\bar{b}) & \xrightarrow{x_0^* \Phi_n} & x_0^* \mathcal{A}_n^{\mathrm{rig}}(\bar{b}) \\ \downarrow \wr & & \downarrow \wr \\ A_n^{\mathrm{dR}}(b_0,x_0) & \xrightarrow{\phi_n(b_0,x_0)} & A_n^{\mathrm{dR}}(b_0,x_0) \end{array} \tag{28}$$

In the computations below, we explicitly determine $\phi_n(b_0,x_0)$ via this diagram, using Lemma 5.1 to characterise the Frobenius structure Φ_n uniquely by its universal property.

5.3. **The Frobenius operator on $A_Z^{\mathrm{dR}}(b,x)$.** After taking the quotient by a choice of a nice correspondence Z, we obtain Frobenius operators

$$\phi_Z(b,x) : A_Z^{\mathrm{dR}}(b,x) \longrightarrow A_Z^{\mathrm{dR}}(b,x)$$

Likewise, we obtain a quotient $\mathcal{A}_Z^{\mathrm{rig}}(\bar{b})$ of the universal 2-step unipotent isocrystal $\mathcal{A}_2^{\mathrm{rig}}(\bar{b})$. Reprising the notation of §5.1, so that in particular $\phi : \mathfrak{U} \longrightarrow \mathfrak{U}$ is an overconvergent lift of Frobenius, Theorem 5.2 gives us an isomorphism

$$\Phi_Z : \phi^* \mathcal{A}_Z^{\mathrm{rig}}(\bar{b}) \xrightarrow{\sim} \mathcal{A}_Z^{\mathrm{rig}}(\bar{b})$$

such that we have a commutative diagram

$$\begin{array}{ccc} x_0^* \mathcal{A}_Z^{\mathrm{rig}}(\bar{b}) & \xrightarrow{x_0^*\Phi_Z} & x_0^* \mathcal{A}_Z^{\mathrm{rig}}(\bar{b}) \\ \downarrow \wr & & \downarrow \wr \\ A_Z^{\mathrm{dR}}(b_0,x_0) & \xrightarrow{\phi_Z(b_0,x_0)} & A_Z^{\mathrm{dR}}(b_0,x_0) \end{array} \tag{29}$$

We have the following two equalities, which will be used to determine $\phi_Z(b,x)$ in practice:

$$\phi_Z(b_0,x_0) = x_0^*\Phi_Z, \qquad \phi_Z(b,x) = \tau_{b,x} \circ \phi_Z(b_0,x_0) \circ \tau_{b,x}^{-1},$$

5.3.1. *Parallel transport.* To compute the isomorphism $\tau_{b,x}$, we use (27). Given an element $(a, \mathbf{b}, c)$ of the algebra $\mathbf{Q}_p \oplus V_{\mathrm{dR}} \oplus \mathbf{Q}_p(1)$, its action via left, respectively right, multiplication is given by

$$\begin{pmatrix} a & 0 & 0 \\ \mathbf{b} & a & 0 \\ c & \mathbf{b}^\intercal Z & a \end{pmatrix}, \qquad \begin{pmatrix} a & 0 & 0 \\ \mathbf{b} & a & 0 \\ c & -\mathbf{b}^\intercal Z & a \end{pmatrix}. \tag{30}$$

When applied to the integrals $\mathbf{I}(x,x_0)$ and $\mathbf{I}(b_0,b)$ from (26), we obtain the matrix describing $\tau_{b,x}$.

5.3.2. *The F-isocrystal $\mathcal{A}_Z^{\mathrm{dR}}(b)^{\mathrm{an}}$.* The connections on $\mathcal{A}_Z^{\mathrm{dR}}(b)^{\mathrm{an}}\,|_Y$ and $\phi^*\,\mathcal{A}_Z^{\mathrm{dR}}(b)^{\mathrm{an}}\,|_Y$ are described with respect to the trivialisation s_0 by equation (20), and are equal to $d+\Lambda$ and $d+\Lambda_\phi$, where

$$\Lambda_\phi = -\begin{pmatrix} 0 & 0 & 0 \\ \phi^*\boldsymbol{\omega} & 0 & 0 \\ \phi^*\eta & \phi^*\boldsymbol{\omega}^\intercal Z & 0 \end{pmatrix}.$$

Henceforth, we set $\phi^*\boldsymbol{\omega} = F\boldsymbol{\omega} + d\mathbf{f}$ for a column vector $\mathbf{f}$ with entries in $\mathrm{H}^0(]Y[, j^\dagger\mathcal{O}_Y)$, uniquely determined by the condition that $\mathbf{f}(b) = \mathbf{0}$. To make the Frobenius structure explicit, we need to find an invertible $(2g+2)\times(2g+2)$-matrix G with entries in $\mathrm{H}^0(]Y[, j^\dagger\mathcal{O}_Y)$, such that

$$\Lambda_\phi G + dG = G\Lambda.$$

Note that G is the inverse of the Frobenius structure, i.e. $G = \Phi_Z^{-1}$. It is a straightforward calculation using the relation $F^\intercal Z F = pZ$ to check that the matrix

$$G = \begin{pmatrix} 1 & 0 & 0 \\ \mathbf{f} & F & 0 \\ h & \mathbf{g}^\intercal & p \end{pmatrix}, \text{ where } \begin{cases} d\mathbf{g}^\intercal &=& d\mathbf{f}^\intercal Z F, \\ dh &=& \boldsymbol{\omega}^\intercal F^\intercal Z \mathbf{f} + d\mathbf{f}^\intercal Z \mathbf{f} - \mathbf{g}^\intercal\boldsymbol{\omega} + \phi^*\eta - p\eta, \\ h(b) &=& 0, \end{cases} \tag{31}$$

induces the required identity. From G, we obtain the Frobenius equivariant isomorphism $s^\phi(b,x)$ as follows. Define

$$s_0(b,x)^{-1} \circ s^\phi(b,x) =: \begin{pmatrix} 1 & 0 & 0 \\ \boldsymbol{\alpha}_\phi(b,x) & 1 & 0 \\ \gamma_\phi(b,x) & \boldsymbol{\beta}_\phi^\intercal(b,x) & 1 \end{pmatrix}.$$

Firstly, since the action of ϕ on $A_Z^{\mathrm{dR}}(b_0, x_0)$ is given by $G(x_0)^{-1}$, we have

$$\begin{pmatrix} 1 & 0 & 0 \\ \boldsymbol{\alpha}_\phi(b_0,x_0) & 1 & 0 \\ \gamma_\phi(b_0,x_0) & \boldsymbol{\beta}_\phi^{\intercal}(b_0,x_0) & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ (I-F)^{-1}\mathbf{f} & 1 & 0 \\ \frac{1}{1-p}\left(\mathbf{g}^{\intercal}(I-F)^{-1}\mathbf{f}+h\right) & \mathbf{g}^{\intercal}(F-p)^{-1} & 1 \end{pmatrix}(x_0).$$

Using the parallel transport formula from Section 5.3.1 we have that

$$\begin{pmatrix} 1 & 0 & 0 \\ \boldsymbol{\alpha}_\phi(b,x) & 1 & 0 \\ \gamma_\phi(b,x) & \boldsymbol{\beta}_\phi^{\intercal}(b,x) & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ \int_x^{x_0}\boldsymbol{\omega} & 1 & 0 \\ \int_x^{x_0}\eta & \int_x^{x_0}\boldsymbol{\omega}^{\intercal}Z & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ \int_{b_0}^{b}\boldsymbol{\omega} & 1 & 0 \\ \int_{b_0}^{b}\eta & -\int_{b_0}^{b}\boldsymbol{\omega}^{\intercal}Z & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ \boldsymbol{\alpha}_\phi(b_0,x_0) & 1 & 0 \\ \gamma_\phi(b_0,x_0) & \boldsymbol{\beta}_\phi^{\intercal}(b_0,x_0) & 1 \end{pmatrix}.$$

5.4. **Computing p-adic heights.** Recall that for the intended Diophantine application, we set out to compute the function

$$\theta \;:\; X(\mathbf{Q}_p) \longrightarrow \mathbf{Q}_p \;;\; x \longmapsto h_p\left(A_Z(b,x)\right)$$

in order to obtain an explicit finite set of points in $X(\mathbf{Q}_p)$ containing $X(\mathbf{Q})$. In §3, we reduced this question to finding an explicit description of the filtered ϕ-module $\mathbf{D}_{\mathrm{cris}}(A_Z(b,x))$.

Lemma 5.3. *There is an isomorphism of filtered ϕ-modules*

$$\mathbf{D}_{\mathrm{cris}}(A_Z(b,x)) \simeq A_Z^{\mathrm{dR}}(b,x).$$

Proof. Olsson's comparison theorem [Ols11, Theorem 1.11] shows that with respect to the Frobenius operator $\phi_n(b,x)$ discussed above, there exist isomorphisms of filtered ϕ-modules

$$\mathbf{D}_{\mathrm{cris}}(A_n^{\text{ét}}(b,x)) \xrightarrow{\sim} A_n^{\mathrm{dR}}(b,x)$$

which on graded pieces $A[n] := \mathrm{Ker}(A_n(b,x) \to A_{n-1}(b,x))$ induces commutative diagrams

$$\begin{array}{ccc} \mathbf{D}_{\mathrm{cris}}(V)^{\otimes n} & \longrightarrow & V_{\mathrm{dR}}^{\otimes n} \\ \downarrow & & \downarrow \\ \mathbf{D}_{\mathrm{cris}}(A[n]) & \longrightarrow & A^{\mathrm{dR}}[n] \end{array}$$

We obtain the following commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbf{D}_{\mathrm{cris}}\left(\mathrm{Coker}\left(\mathbf{Q}_p(1) \xrightarrow{\cup^*} V^{\otimes 2}\right)\right) & \longrightarrow & \mathbf{D}_{\mathrm{cris}}(A_2^{\text{ét}}(b,x)) & \longrightarrow & \mathbf{D}_{\mathrm{cris}}(A_1^{\text{ét}}(b,x)) & \longrightarrow & 0 \\ & & \downarrow \wr & & \downarrow \wr & & \downarrow \wr & & \\ 0 & \longrightarrow & \mathrm{Coker}\left(\mathbf{Q}_p(1) \xrightarrow{\cup^*} V_{\mathrm{dR}}^{\otimes 2}\right) & \longrightarrow & A_2^{\mathrm{dR}}(b,x) & \longrightarrow & A_1^{\mathrm{dR}}(b,x) & \longrightarrow & 0 \end{array} \tag{32}$$

It follows that $\mathbf{D}_{\mathrm{cris}}(A_Z(b,x))$ may be identified with the filtered ϕ-module $A_Z^{\mathrm{dR}}(b,x)$ obtained by pushing out the bottom exact sequence of diagram (32) by the map

$$\mathrm{cl}_Z^* : V_{\mathrm{dR}} \otimes V_{\mathrm{dR}} \longrightarrow \mathbf{Q}_p(1),$$

where we implicitly use the fact that the p-adic comparison isomorphism is compatible with cycle class maps, and the fact that cl_Z^* factors through $\mathrm{Coker}(\cup^*)$. □

Recall that in §4, we obtained a simple algorithm for determining the Hodge filtration on $\mathcal{A}_Z(b)$ via Hadian's universal property. The Frobenius structure is computed explicitly on the Teichmüller representative x_0 of x using the algorithms of Tuitman [Tui16, Tui17] to solve the system of equation

(31), and then for x via explicit integration in the residue disk. The steps outlined at the end of 4.5 and 5.3 yield matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \gamma_{\mathrm{Fil}}(b,x) & \boldsymbol{\beta}_{\mathrm{Fil}}^{\intercal}(b) & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 \\ \boldsymbol{\alpha}_\phi(b,x) & 1 & 0 \\ \gamma_\phi(b,x) & \boldsymbol{\beta}_\phi^{\intercal}(b,x) & 1 \end{pmatrix}$$

As an immediate consequence of equation (15), we obtain from Lemma 5.3 the following result.

Lemma 5.4. *For any $x \in X(\mathbf{Q}_p) \cap\,]\mathcal{U}[$, the local p-adic height of $A_Z(b,x)$ is given by*

$$h_p(A_Z(b,x)) = \chi_p\left(\gamma_\phi(b,x) - \gamma_{\mathrm{Fil}}(b,x) - \boldsymbol{\beta}_\phi^{\intercal}(b,x)\cdot s_1(\boldsymbol{\alpha}_\phi)(b,x) - \boldsymbol{\beta}_{\mathrm{Fil}}^{\intercal}(b)\cdot s_2(\boldsymbol{\alpha}_\phi)(b,x)\right).$$

Remark 5.5. We also deduce the following formula for the p-adic Abel–Jacobi class of the Chow–Heegner point $[IA_Z(b)]$ discussed in Remark 3.10. Let C denote the matrix describing the cup product, then

$$[IA_Z(b)] = C\cdot(\boldsymbol{\beta}_\phi(b,b) - \boldsymbol{\beta}_{\mathrm{Fil}}(b)), \tag{33}$$

5.5. **A trick for dealing with leftover residue disks.** The process described above gives a way of computing a finite set containing $X(\mathbf{Q})\cap]\mathcal{U}[$. This leaves the residue disks where the Frobenius lift is not defined, or where the basis differentials have poles. To deal with those residue disks, we could pass to a different choice of basis and Frobenius lift until the whole of X is covered.

An alternative approach is to change the base point, which may be of some independent interest. Suppose $b' \in X(\mathbf{Q})$ lies in a residue disk where none of our basis differentials have poles. The starting point is the observation that the set $X(\mathbf{Q}_p)_{\mathrm{U}}$ is independent of b'. The computation in §4.5 of the Hodge filtration is largely independent of the base point, yielding

$$\begin{cases} \boldsymbol{\beta}_{\mathrm{Fil}}^{\intercal}(b') &= \boldsymbol{\beta}_{\mathrm{Fil}}^{\intercal}(b) \\ \gamma_{\mathrm{Fil}}(b',x) &= \gamma_{\mathrm{Fil}}(b,x) - \gamma_{\mathrm{Fil}}(b,b'). \end{cases} \tag{34}$$

The effect of changing the base point on the Frobenius structure is described by the following lemma.

Lemma 5.6. *Let $b' \in X(\mathbf{Q}_p)$ lie on a residue disk where none of the basis differentials have poles. Then*

$$s_0^{-1}(b',b')\circ s^\phi(b',b') = \begin{pmatrix} 1 & 0 & 0 \\ \boldsymbol{\alpha}_\phi(b',b') & 1 & 0 \\ \gamma_\phi(b',b') & \boldsymbol{\beta}_\phi^{\intercal}(b',b') & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \boldsymbol{\beta}_\phi^{\intercal}(b,b) + 2\int_b^{b'}\boldsymbol{\omega}^{\intercal}Z & 1 \end{pmatrix}.$$

Proof. Recall that we defined the Frobenius structure on $A_Z(b',b')$ via the quotient map

$$A_2^{\mathrm{dR}}(Y)(b',b') \longrightarrow A_Z^{\mathrm{dR}}(b',b').$$

By equation (27), there is a ϕ-equivariant unipotent isomorphism

$$\begin{array}{ccc} A_n^{\mathrm{dR}}(Y)(b,b) & \longrightarrow & A_n^{\mathrm{dR}}(Y)(b',b') \\ s_0(b,b)(v) & \longmapsto & s_0(b',b')\,(\,\mathbf{I}(b,b')v\mathbf{I}(b',b)\,)\,. \end{array} \tag{35}$$

To apply equation (35), we first have to describe the algebra structure of $A_Z^{\mathrm{dR}}(b,b)$ thought of as a quotient of $A_2^{\mathrm{dR}}(b,b)$. By equations (30) and (35), we obtain that $s_0^{-1}(b',b')\circ s^\phi(b',b')$ is equal to

$$\begin{pmatrix} 1 & 0 & 0 \\ \int_b^{b'}\boldsymbol{\omega} & 1 & 0 \\ \int_b^{b'}\eta + \int_b^{b'}\boldsymbol{\omega}^{\intercal}Z\boldsymbol{\omega} & \int_b^{b'}\boldsymbol{\omega}^{\intercal}Z & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ \int_b^{b'}\boldsymbol{\omega} & 1 & 0 \\ \int_b^{b'}\eta + \int_b^{b'}\boldsymbol{\omega}^{\intercal}Z\boldsymbol{\omega} & -\int_b^{b'}\boldsymbol{\omega}^{\intercal}Z & 1 \end{pmatrix}^{-1}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \boldsymbol{\beta}_\phi^{\intercal}(b,b) & 1 \end{pmatrix},$$

using the composition of Frobenius equivariant isomorphisms

$$\mathbf{Q}_p \oplus V_{\mathrm{dR}} \oplus \mathbf{Q}_p(1) \xrightarrow{\simeq} A_Z(b,b) \xrightarrow{\simeq} A_Z(b',b) \xrightarrow{\simeq} A_Z(b',b').$$

□

6. Example: $X_s(13)$

As in the introduction, we denote by $X_{\mathrm{s}}(\ell)$ the modular curve associated to the normaliser of a split Cartan subgroup of $\mathrm{GL}_2(\mathbf{F}_\ell)$, where ℓ is a prime number. This curve can be defined over $\mathbf{Q}$ and there is a $\mathbf{Q}$-isomorphism $X_0^+(\ell^2) \simeq X_{\mathrm{s}}(\ell)$ coming from conjugation with $\left(\begin{smallmatrix}\ell & 0\\ 0 & 1\end{smallmatrix}\right)$, where $X_0^+(\ell^2)$ is the quotient of $X_0(\ell^2)$ by the Atkin-Lehner involution w_{ℓ^2}.

In this section, we compute the rational points on $X = X_{\mathrm{s}}(13)$, which is a curve of genus 3. We show in §6.1 that we have $\rho(\mathrm{J}_{\mathbf{Q}}) = 3 = \mathrm{rk}(\mathrm{J}/\mathbf{Q})$ and in §6.2 that X has potentially good reduction everywhere. Hence Corollary 3.7 implies that

$$\Upsilon_Z = (\theta_Z, \{0\})$$

is a quadratic Chabauty pair for X, where $Z \in \mathrm{Pic}(X \times X) \otimes \mathbf{Q}_p$ is nice and $\theta_Z(x) = h_p(A_Z(b, x))$.

We work at the prime $p = 17$ and we choose $g + \rho - 1 - r = 2$ independent nice Z; by Lemma 1.5 we get two finite sets of 17-adic points which contain $X(\mathbf{Q})$. Their intersection turns out to be exactly $X(\mathbf{Q})$, which proves Theorem 1.1.

Remark 6.1. The choice of the prime 17 is somewhat arbitrary. For primes less than 11, our chosen basis of de Rham cohomology is not p-integral, and at $p = 13$ the curve has bad reduction.

6.1. **Ranks.** Modular symbol routines as implemented in `Magma` [BCP97] allow us to compute the space of weight 2 cuspforms for $\Gamma_0^+(169)$, and it turns out that their eigenforms form a single Galois conjugacy class defined over $\mathbf{Q}(\zeta_7)^+$. An explicit eigenbasis is given by the Galois conjugates of the form f, with q-expansion

$$f = q + \alpha q^2 + (-\alpha^2 - 2\alpha)q^3 + (\alpha^2 - 2)q^4 + (\alpha^2 + 2\alpha - 2)q^5 + (-\alpha - 1)q^6 + \dots,$$

where α is a root of $x^3 + 2x^2 - x - 1$. We conclude by [Shi70, Theorem 7.14] and [Rib80, Corollary 4.2] that $\mathrm{End}(\mathrm{J}) \otimes \mathbf{Q} \simeq K := \mathbf{Q}(\zeta_7)^+$, and J is a simple abelian threefold. Therefore $\rho(\mathrm{J}_{\mathbf{Q}}) = 3$.

Proposition 6.2. *We have* $\mathrm{rk}(\mathrm{J}/\mathbf{Q}) = 3$.

Proof. Let A_f denote the modular abelian variety $A_f = J_0(169)/I_f$ associated to f, where I_f is the annihilator of f in the Hecke algebra $\mathbb{T}$ acting on $J_0(169)$. Then A_f is an optimal quotient of $J_0(169)$ in the sense that the kernel of $J_0(169) \to A_f$ is connected. Since J is $\mathbf{Q}$-isogenous to A_f (this was already used by Baran in [Bar14b]), it suffices to show that $\mathrm{rk}(A_f/\mathbf{Q}) = 3$. The work of Gross-Zagier [GZ86] and Kolyvagin-Logachev [KL89] proves that if the order of vanishing of the L-function $L(f, s)$ of f at $s = 1$ is 1, then $\mathrm{rk}(A_f/\mathbf{Q}) = g = 3$.

We showed that $\mathrm{ord}_{s=1} L(f, s) > 0$ by computing the eigenvalue of f under the Fricke involution W_{169} and by computing the rational number $c_{A_f} L(f, 1)/\Omega_{A_f}$ exactly using the algorithm of [AS05], where c_{A_f} is the Manin constant of A_f and Ω_{A_f} is the real period. So it only remains to show that $L'(f, 1) \neq 0$, which we did using `Magma`. We found that the number $L'(f, 1)$ was always larger than 0.6 for any embedding $\mathbf{Q}(\alpha) \hookrightarrow \mathbb{C}$ and the error in these computations was smaller than 10^{-100}. □

Remark 6.3. An alternative approach was explained to us by Schoof [Sch12]. The computation of the rank using descent is discussed by Bruin, Poonen and Stoll in [BPS16]. They show that the rank is at least 3 by exhibiting three rational points in J which are independent modulo torsion. To carry out the descent needed to bound the rank from above, one needs to compute the class group of a certain number field L of degree 28 and discriminant $2^{42} \cdot 13^{12}$. In [BPS16], this enables the authors to compute the rank assuming the Generalized Riemann Hypothesis. The authors of [BPS16] suggest that "the truly dedicated enthusiast could probably verify unconditionally that the class group of $\mathcal{O}_L$ is trivial."

6.2. **Semi-stable reduction of $X_{\mathrm{s}}(\ell)$.** We show that $X_{\mathrm{s}}(13)$ has potentially good reduction by computing, more generally, semi-stable models of the split Cartan modular curves $X_{\mathrm{s}}(\ell)$ for primes $\ell \equiv 1 \pmod{12}$ over the integers in an explicit extension of $\mathbf{Q}_\ell$, using the work of Edixhoven [Edi89, Edi90]. For the remainder of this subsection, we let ℓ denote a prime number of the form $\ell = 12k+1$.

Remark 6.4. For simplicity, we restrict to the case $\ell \equiv 1 \pmod{12}$, when there are no supersingular elliptic curves with j-invariant 0 or 1728. The same analysis would work in general if one in addition makes the action of the additional automorphisms explicit, which is done in [Edi89, §2.1.3]. We also note that additional level structure away from ℓ has little effect on our analysis, and may easily be included, mutatis mutandis.

For a Dedekind domain R we say $\phi : \mathcal{X} \to \operatorname{Spec} R$ is a *model* for a smooth, proper, geometrically connected curve X over the field of fractions of R if ϕ is proper and flat, $\mathcal{X}$ is integral and normal, and the generic fibre of $\mathcal{X}$ is isomorphic to X over the base field. Such a model is called *semi-stable* if all its geometric fibres are reduced and have at most ordinary double points as singularities. In what follows, we set W to be the ring of Witt vectors over $\overline{\mathbf{F}}_\ell$, with field of fractions $\mathbf{Q}_\ell^{\mathrm{nr}}$. Furthermore, we set $\mathrm{Ig}(\ell)$ to be the *Igusa curve*, which is the coarse moduli space over $\overline{\mathbf{F}}_\ell$ classifying elliptic curves $E \to S/\overline{\mathbf{F}}_\ell$ together with $\Gamma_1(\ell)$-Drinfeld level structure on $E^{(\ell)}$ which generates the kernel of the Verschiebung map $V : E^{(\ell)} \to E$, see [KM85, Section 12.3].

We start by recalling the work of Edixhoven on the semi-stable reduction of $X_0(\ell^2)$. The description of the model may be found in [Edi90], and the statements about w_{ℓ^2} are in [Edi89, §2.2, 2.3.4].

Theorem 6.5 (Edixhoven)**.** *The curve $X_0(\ell^2)$ obtains semi-stable reduction over $\mathbf{Q}_\ell^{\mathrm{nr}}(\varpi)$, where ϖ is such that $\varpi^{12k(6k+1)} = \ell$. Its special fibre consists of the following components:*

- *k **horizontal** components, all isomorphic to $u^2 = v^{\ell+1} + 1$.*
- *Four **vertical** components, of which two are rational, and two are isomorphic to $\mathrm{Ig}(\ell)/\pm 1$.*

Every horizontal component intersects every vertical component exactly once, and there are no other intersections. The Atkin–Lehner operator w_{ℓ^2} stabilises every horizontal component, and acts via $(u, v) \longmapsto (u, -v)$ in the above coordinates. Furthermore, w_{ℓ^2} permutes the rational vertical components, and stabilises the Igusa curves.

We write $\mathcal{X}$ for this semi-stable model of $X_0(\ell^2)$ over $W[\varpi]$. We denote the maximal ideal of $W[\varpi]$ by $\mathfrak{m}$, and for any scheme $\mathcal{Y}$ over $W[\varpi]$, we write $\mathcal{Y}_s$ for its special fibre.

Theorem 6.6. *The curve $X_{\mathrm{s}}(\ell)$ obtains semi-stable reduction over the field $\mathbf{Q}_\ell^{\mathrm{nr}}(\varpi)$, where $\varpi^{\ell^2-1} = \ell^2$. There exists a semi-stable model, whose special fibre consists of the following components:*

- *k **horizontal** components, all isomorphic to $u^2 = v^{6k+1} + 1$.*
- *Three **vertical** components, of which one is rational, and two are isomorphic to $\mathrm{Ig}(\ell)/\mathrm{C}_4$.*

Every horizontal component intersects every vertical component exactly once, and there are no other intersections.

Proof. Because $X_0^+(\ell^2) \simeq_{\mathbf{Q}} X_{\mathrm{s}}(\ell)$, it follows from [Ray90, Proposition 5] that the quotient $\mathcal{X}^+ = \mathcal{X}/w_{\ell^2}$ is a semi-stable model for $X_{\mathrm{s}}(\ell)$. To describe the special fibre of this model, note that the order of w_{ℓ^2} is invertible on $\mathcal{O}_{\mathcal{X}}$, and we therefore have

$$\mathrm{H}^1\left(\langle w_{\ell^2}\rangle, \mathfrak{m}\right) = 0.$$

This implies that $\mathcal{O}_{\mathcal{X}^+}/\mathfrak{m} \simeq (\mathcal{O}_{\mathcal{X}}/\mathfrak{m})^{w_{\ell^2}}$, and hence $\mathcal{X}_s^+ = \mathcal{X}_s/w_{\ell^2}$. The description of the special fibre follows from that of the action of w_{ℓ^2} in Theorem 6.5. First, we note that both rational components of $\mathcal{X}_s$ are identified by w_{ℓ^2}, giving rise to a unique rational component in the quotient. By [Edi89, §2.2], the quotients of the non-rational vertical components are isomorphic to the Igusa

curves $\mathrm{Ig}(\ell)/\mathrm{C}_4$, which are of genus $(k-1)(3k-2)/2$, whereas the quotients of the horizontal components have equation $u^2 = v^{6k+1} + 1$, and are hence of genus $3k$. The result follows. □

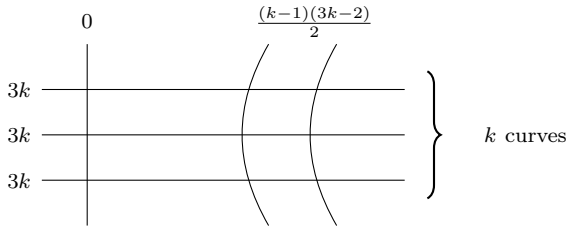

FIGURE 1. Reduction of the semi-stable model of $X_{\mathrm{s}}(\ell)$.

As a consequence, we obtain the genus formula $g = 6k^2 - 3k$ for the curve $X_{\mathrm{s}}(\ell)$.

Corollary 6.7. *The split Cartan modular curve $X_{\mathrm{s}}(13)$ has good reduction outside 13, and potentially good reduction at 13. More precisely, it obtains good reduction over the field $\mathbf{Q}_{13}^{\mathrm{nr}}(\varpi)$, where $\varpi^{84} = 13$.*

Proof. The result follows from Theorem 6.6. Indeed, we may contract all three rational curves to obtain a smooth model over $W[\varpi]$. □

Remark 6.8. Since $X_{\mathrm{ns}}(13) \simeq X_{\mathrm{s}}(13)$, the same result holds for the non-split curve of level 13.

6.3. **Defining equations and known rational points.** Baran [Bar14a] finds an explicit defining equation for $X_{\mathrm{s}}(13)$ as follows. As the curve $X_{\mathrm{s}}(13) \simeq X_0^+(169)$ is of genus 3, it is either hyperelliptic or has a smooth plane quartic model. It may be checked that the q-expansions of the Galois conjugates of f do not satisfy a quadratic relation, but do satisfy a quartic relation, resulting in the plane model[2]

$$(-Y - Z)X^3 + (2Y^2 + YZ)X^2 + (-Y^3 + Y^2Z - 2YZ^2 + Z^3)X + (2Y^2Z^2 - 3YZ^3) = 0,$$

which has good reduction away from 13. To apply the algorithms of [Tui16, Tui17], it will be convenient to have a plane quartic model whose Y^4-coefficient is 1. For this reason we apply the substitution $(X : Y : Z) \mapsto (X - Y : X + Y : X + Z)$ giving the model $Q(X, Y, Z) = 0$, where

$$\begin{aligned} Q(X,Y,Z) = {} & Y^4 + 5X^4 - 6X^2Y^2 + 6X^3Z + 26X^2YZ + 10XY^2Z - 10Y^3Z - 32X^2Z^2 - 40XYZ^2 \\ & + 24Y^2Z^2 + 32XZ^3 - 16YZ^3 \end{aligned}$$

which we will use henceforth and which has good reduction away from 2 and 13. With respect to this model, the 7 known rational points are as follows:

P_0	P_1	P_2	P_3	P_4	P_5	P_6
$(1:1:1)$	$(1:1:2)$	$(0:0:1)$	$(-3:3:2)$	$(1:1:0)$	$(0:2:1)$	$(-1:1:0)$

In the remainder of this section, we show that there are no other rational points on X.

6.4. **Finding rational points on the first affine chart.** Set Y to be the affine chart $Z \neq 0$ with respect to the model $Q = 0$, with coordinates $x = X/Z$, $y = Y/Z$. Then Y contains all known rational

[2]Hopefully, no confusion will arise from our use of the letters X, Y and Z, which also denote other objects in this paper, as projective coordinates.

points, except P_4 and P_6. Let us choose the basepoint to be $b = P_2 = (0,0)$. Define $Q_y = \partial Q/\partial y$, then a set of differentials which satisfy all the properties in §4.1 is given by

$$\boldsymbol{\omega} := \begin{pmatrix} 1 \\ x \\ y \\ -160x^4/3 + 736x^3/3 - 16x^2y/3 + 436x^2/3 - 440xy/3 + 68y^2/3 \\ -80x^3/3 + 44x^2 - 40xy/3 + 68y^2/3 - 32 \\ -16x^2y + 28x^2 + 72xy - 4y^2 - 160x/3 + 272/3 \end{pmatrix} \frac{dx}{Q_y}.$$

We construct p-adic de Rham classes as in §4.4 associated to nice correspondences as follows: If q is a prime of good reduction, and if ι denotes the inclusion of $K \otimes \mathbf{Q}_q$ into $\mathrm{End}(\mathrm{H}^1_{\mathrm{dR}}(X_{\mathbf{Q}_q}))$, then by Eichler-Shimura the action of the Hecke operator T_q on $\mathrm{H}^1_{\mathrm{dR}}(X_{\mathbf{Q}_q})$ is given by

$$\iota(a_q)(f) = \mathrm{Fr}_q + q\,\mathrm{Fr}_q^{-1}, \tag{36}$$

Using the algorithms of [Tui16, Tui17], we can compute the matrix of Fr_q with respect to the basis $\boldsymbol{\omega}$ to any desired precision. Then (36) allows us to compute the matrix A_q of T_q with respect to $\boldsymbol{\omega}$, and multiplying $6A_q - \mathrm{tr}(A_q)I_6$ by the inverse of the cup product matrix with respect to $\boldsymbol{\omega}$, we obtain

$$Z_1 = \begin{pmatrix} 0 & -976 & -1104 & 10 & -6 & 18 \\ 976 & 0 & -816 & -3 & 1 & 3 \\ 1104 & 816 & 0 & -3 & 3 & -11 \\ -10 & 3 & 3 & 0 & 0 & 0 \\ 6 & -1 & -3 & 0 & 0 & 0 \\ -18 & -3 & 11 & 0 & 0 & 0 \end{pmatrix}, \qquad Z_2 = \begin{pmatrix} 0 & 112 & -656 & -6 & 6 & 6 \\ -112 & 0 & -2576 & 15 & 9 & 27 \\ 656 & 2576 & 0 & 3 & 3 & -3 \\ 6 & -15 & -3 & 0 & 0 & 0 \\ -6 & -9 & -3 & 0 & 0 & 0 \\ -6 & -27 & 3 & 0 & 0 & 0 \end{pmatrix}$$

using $q = 7$ and $q = 11$, respectively. These matrices encode independent Tate classes $Z_1, Z_2 \in \mathrm{H}^1_{\mathrm{dR}}(X) \otimes \mathrm{H}^1_{\mathrm{dR}}(X)$ with respect to the basis $\boldsymbol{\omega}$, which satisfy the conditions (a) – (d) of §4.4.

We find that a basis of $\mathrm{H}^0(X, \mathcal{O}(2D))$ is given by $1, x, y, x^2, xy, y^2$, where $D = X \setminus Y$. Using the algorithm outlined after Lemma 4.7, we compute the Hodge filtration of the connections $\mathcal{A}_{Z_i}$:

$$\begin{array}{lcllcl} \eta_{Z_1} & = & -(44x^2 + 148/3xy + 8y^2)\frac{dx}{Q_y} & \eta_{Z_2} & = & -(40x^2 + 148xy + 36y^2)\frac{dx}{Q_y} \\ \boldsymbol{\beta}_{\mathrm{Fil},Z_1} & = & (0, 1/2, 1/2)^\intercal & \boldsymbol{\beta}_{\mathrm{Fil},Z_2} & = & (0, -1/2, -5/2)^\intercal \\ \gamma_{\mathrm{Fil},Z_1} & = & 5y/6 + 3x/2 & \gamma_{\mathrm{Fil},Z_2} & = & -5y/6 - 15x/2. \end{array}$$

Define $\mathcal{U}_1 := Y_{\mathbf{F}_p} \cap \{Q_y \neq 0\}$. We apply the methods of [Tui16] to define a lift Φ of Frobenius on a strict open neighbourhood of $]\mathcal{U}_1[$ satisfying $\Phi(x) = x^p$. The base point $b = P_2$ is a Teichmüller point with respect to our chosen Φ. The Frobenius structure of $\mathcal{A}^{\mathrm{rig}}_{Z_i}$ is determined using the techniques of §5.3. This enables us to compute θ_{Z_1} and θ_{Z_2} as a power series on every residue disk in $]\mathcal{U}_1[$ via Lemma 5.4.

6.4.1. *Equivariant p-adic heights and quadratic Chabauty pairs.* Having computed the Hodge filtration and Frobenius structure for Z_1 and Z_2, we now explain how to compute the function in Lemma 1.5 for the quadratic Chabauty pairs associated to Z_1 and Z_2, respectively. First, we can compute the action of K on $\mathrm{H}^1_{\mathrm{dR}}(X)$ by noting that $a_3 := a_3(f) = -\alpha^2 - 2\alpha$ generates K and by computing the action $\iota(a_3)$ of the Hecke operator T_3 on $\mathrm{H}^1_{\mathrm{dR}}(X)$ using (36). This enables us to compute a K-equivariant splitting s of the Hodge filtration on $\mathrm{H}^1_{\mathrm{dR}}(X)$; by Remark 3.8, the p-adic height h taken with respect to s is K-equivariant. Finally, as in the introduction we set $K_p = K \otimes \mathbf{Q}_p$ and

$$\mathcal{E} = \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^* \otimes_{K_p} \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^*.$$

By Lemma 3.6, we need to consider, for $x \in X(\mathbf{Q}_p)$ and $Z \in \{Z_1, Z_2\}$, the extensions

$$E_1(x) := E_1(A_Z(b,x)) = \mathrm{AJ}_b(x), \qquad E_{2,Z}(x) := E_2(A_Z(b,x)) = E(\mathrm{AJ}_b(x)) + c,$$

with notation as in (11), viewed as elements of $\mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^*$. We start by computing $E_1(P_i)$ and $E_{2,Z}(P_i)$ for the known points P_1, P_2, P_3, P_5 in $]\mathcal{U}_1[\cap X(\mathbf{Q})$ from the Hodge filtration and Frobenius structure of $A_Z(b, P_i)$. We find that $E_1(P_5)$ is nonzero, and hence generates $\mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^*$ over K_p. Moreover, we compute that the elements

$$\iota(a_3)^i \left(E_1(P_5) \otimes_{K_p} E_{2,Z_1}(P_5)\right), \qquad i = 0, 1, 2$$

are a $\mathbf{Q}_p$-basis for $\mathcal{E}$, and we define ψ_1, ψ_2, ψ_3 to be the dual basis of $\mathcal{E}^*$. We also find that

$$\begin{aligned} E_1(P_1) \otimes_{K_p} E_{2,Z_1}(P_1) &= \iota(3164 + 1994\alpha + 294\alpha^2)\left(E_1(P_5) \otimes_{K_p} E_1(P_5)\right) \\ E_1(P_3) \otimes_{K_p} E_{2,Z_1}(P_3) &= \iota(1574 + 1006\alpha + 150\alpha^2)\left(E_1(P_5) \otimes_{K_p} E_1(P_5)\right) \\ E_1(P_5) \otimes_{K_p} E_{2,Z_1}(P_5) &= \iota(-232 - 134\alpha - 18\alpha^2)\left(E_1(P_5) \otimes_{K_p} E_1(P_5)\right) \end{aligned}$$

so that the three classes on the left form a basis for $\mathcal{E}$. By Lemma 1.5 and 3.6, this gives two matrices

$$T_i(x) := \begin{pmatrix} \theta_{Z_i}(x) & \Psi_1(Z_i\ , x) & \Psi_2(Z_i\ , x) & \Psi_3(Z_i\ , x) \\ \theta_{Z_1}(P_1) & \Psi_1(Z_1, P_1) & \Psi_2(Z_1, P_1) & \Psi_3(Z_1, P_1) \\ \theta_{Z_1}(P_3) & \Psi_1(Z_1, P_3) & \Psi_2(Z_1, P_3) & \Psi_3(Z_1, P_3) \\ \theta_{Z_1}(P_5) & \Psi_1(Z_1, P_5) & \Psi_2(Z_1, P_5) & \Psi_3(Z_1, P_5) \end{pmatrix}, \qquad \Psi_j(Z, z) := \psi_j(E_1(z) \otimes_{K_p} E_{2,Z}(z)),$$

such that the locally analytic functions $\det(T_i(x)) : X(\mathbf{Q}_p) \to \mathbf{Q}_p$ vanish on $X(\mathbf{Q}_p)_2$. It only remains to determine their common zeroes. This may be done by computing up to high enough precision, in the following sense. Let $F_i \in \mathbf{Z}_p[\![t]\!]$, and suppose

$$G(t) = \sum_{n \geq 0} c_n t^n = \sum a_{ij} \int F_i \left(\int F_j \right) + \sum a_i \int F_i + \sum b_i F_i$$

is a $\mathbf{Q}_p$-linear combination of the F_i, their single integrals, and their double integrals. An elementary estimate gives us

$$v_p(c_n) \geq \min\left\{v_p(a_i), v_p(a_{ij}), v_p(b_i)\right\}_{i,j} - 2\lfloor \log_p(n) \rfloor,$$

so that if we compute enough coefficients for the power series F_i, the slopes of the Newton polygon of $G(t)$ beyond our precision are bounded below by -1, and can hence not come from $\mathbf{Q}_p$-rational points. A table of the zeroes of $\det(T_1(x))$ and $\det(T_2(x))$ on $]\mathcal{U}_1[$ may be found in [BDM+]. All zeroes of $\det(T_1(x))$ and $\det(T_2(x))$ are simple, and the only simultaneous zeroes are P_1, P_2, P_3 and P_5. Hence these are the only $\mathbf{Q}$-rational points on $]\mathcal{U}_1[$.

Remark 6.9. Note that by construction $\det(T_1(x))$ vanishes on P_1, P_3, P_5. However, the rational point P_2 was not used as input, so that the vanishing of $\det(T_1(x))$ on P_2 provides an independent check. Even more strikingly, the vanishing of $\det(T_2(x))$ at *none* of the points P_1, P_2, P_3, P_5 is automatic, which seems to us an extremely convincing confirmation of the correctness of our algorithms.

6.5. **Rational points on $]\mathcal{U}_2[$.** We now consider a second affine chart Y' defined by $X \neq 0$ with respect to the model $Q = 0$, with coordinates $u := Z/X$ and $v := Y/X$. Then Y' contains all known rational points, except P_2 and P_5. Let us choose the basepoint to be $b = P_6 = (0, -1)$. One may similarly write down a basis of differentials in terms of u and v, which satisfy all the properties in §4.1 with respect to Y', and are cohomologous to the previous differentials $\boldsymbol{\omega}$ in $\mathrm{H}^1_{\mathrm{dR}}(X)$, so that the matrices Z_1 and Z_2 remain unchanged. The exact details of the basis we use may be found in [BDM+].

We calculated the Hodge filtration using the algorithm outlined after Lemma 4.7. To compute the Frobenius structure, define $\mathcal{U}_2 := Y'_{\mathbf{F}_p} \cap \{Q_v \neq 0\}$. As our model is monic in v, we can again apply the methods of [Tui16] to define a lift Φ of Frobenius on a strict open neighbourhood of $]\mathcal{U}_2[$ satisfying $\Phi(u) = u^p$. The base point $b = P_6$ is a Teichmüller point with respect to our chosen Φ. The Frobenius structure of $\mathcal{A}^{\mathrm{rig}}_{Z_i}$ is determined using the techniques of §5.3. This enables us to compute θ_{Z_1} and θ_{Z_2} as a power series on every residue disk in $]\mathcal{U}_2[$ via Lemma 5.4.

Using the same rational points as we did in the previous section, we construct two matrices $T_i'(u)$, whose determinant vanishes at all the rational points on $]\mathcal{U}_2[$. It suffices to check the residue disks of $(1:1:0)$, $(1:-1:0)$ and $(1:1:1)$. The Frobenius lift we chose was not defined on the residue disk of $(1:1:1)$, but for the other two disks we obtain the zeroes of $\det(T_1'(u))$ and $\det(T_2(u'))$ to precision $O(17^5)$, see [BDM+]. All zeroes are simple and the only points which are simultaneous zeroes are $(0,1)$ and $(0,-1)$. Combined with the calculations of §6.4, this shows that there are no points in $X(\mathbf{Q})$ besides the known ones, except perhaps on the residue disk of $(1:1:1)$.

6.6. **Rational points on $](1:1:1)[$.** The remaining residue disk lies at the point $P_0 = (1:1:1)$, which was the disk where the Frobenius lift above is not defined. Rather than choosing a new lift of Frobenius, as explained in §5.5 we may use Lemma 5.6 to reduce the computation of p-adic heights of $A_Z(P_0, x)$, for x in $]P_0[$, to the problem of computing the single integrals $\int_b^{P_0} \boldsymbol{\omega}$ These integrals are computed using the original Frobenius lift, via overconvergence and evaluating at points defined over highly ramified extensions of $\mathbf{Q}_p$ (see [BT17, Prop 3.8, Prop 4.3]). We find that, for both choices of Z, the only roots of the resulting power series are at $P_0 = (1:1:1)$ (and are simple). This completes the proof of Theorem 1.1.

Appendix A. Universal objects and unipotent isocrystals

In this appendix, we briefly discuss the notion of universal objects in unipotent Tannakian categories, and discuss them in the example of the category of unipotent isocrystals on $\mathcal{X}_{\mathbf{F}_p}$.

A.1. **Universal objects in unipotent Tannakian categories.** We say a neutral Tannakian category $\mathcal{C}$ is *unipotent* if its fundamental group is pro-unipotent. For a general unipotent neutral Tannakian category $\mathcal{C}$ with fibre functors ω and ν, we first define universal objects $\mathcal{A}_n(\mathcal{C}, \omega)$. Their utility comes from the fact that one can often compute 'extra structure' on fundamental groups and path torsors by instead computing that extra structure on certain universal objects in the category.

It is instructive to first consider the case of fundamental groups of topological spaces. If X is a locally path connected topological space, with universal cover $\widetilde{X}$, then there is a well known correspondence between deck transformations of $\widetilde{X}$ and elements of the fundamental group. This is perhaps most naturally formulated by replacing the universal cover with a *pointed* universal cover

$$p : (\widetilde{X}, \widetilde{b}) \longrightarrow (X, b).$$

Then the correspondence is given by the statement that the following map is bijective:

$$\pi_1(X, b) \longrightarrow p^{-1}(\{b\}), \quad \gamma \longmapsto \gamma(\widetilde{b}).$$

A.1.1. *Universal objects.* Similar universal objects may be constructed in certain Tannakian categories. For the main definitions on Tannakian categories and their fundamental groups, we refer to Deligne [Del90], and will make free use of the language introduced there.

Definition A.1. *We say a neutral Tannakian category $\mathcal{C}$ over a field K with fibre functor ω is unipotent if its fundamental group $\pi_1(\mathcal{C}, \omega)$ is pro-unipotent. Equivalently, $\mathcal{C}$ is unipotent if every object $V \in \mathcal{C}$ admits a nonzero morphism $\mathbf{1} \longrightarrow V$ from the unit object $\mathbf{1}$ in $\mathcal{C}$.*

Let $\mathcal{C}$ be a neutral unipotent Tannakian category over a field K of characteristic zero, with fibre functor ω, let $A(\mathcal{C}, \omega)$ denote its pro-universal enveloping algebra, with augmentation ideal I, and define $A_n(\mathcal{C}, \omega) := A(\mathcal{C}, \omega)/I^{n+1}$. Recall that there is a canonical isomorphism

$$\varinjlim_n A_n(\mathcal{C}, \omega)^* \xrightarrow{\sim} \mathcal{O}(\pi_1(\mathcal{C}, \omega))$$

between the dual Hopf algebra and the co-ordinate ring of the affine group scheme $\pi_1(\mathcal{C},\omega)$. Since $A_n(\mathcal{C};\omega)$ is a finite dimensional K-representation of $\pi_1(\mathcal{C},\omega)$, it corresponds by Tannaka duality to an object $\mathcal{A}_n(\mathcal{C},\omega)$ of the category $\mathcal{C}$, with the property that $\omega(\mathcal{A}_n(\mathcal{C},\omega)) = A_n(\mathcal{C},\omega)$.

Now suppose $(\mathcal{C},\omega)$ has finite dimensional Ext-groups. A *pointed object* in $\mathcal{C}$ is a pair (V,v) where $V \in \mathcal{C}$ and $v \in \omega(V)$. An object of $\mathcal{C}$ is *n-unipotent* if there exists a filtration

$$V = V_0 \supset \ldots \supset V_n$$

by subobjects such that V_i/V_{i+1} is zero or is isomorphic to a direct sum of copies of the trivial object, for all i. A morphism between pointed n-unipotent objects is a morphism in $\mathcal{C}$ that respects the filtrations V_i, and the chosen vectors v.

Definition A.2. *We say a pointed n-unipotent object $(\mathcal{E},e)$ is a universal pointed n-unipotent object if for all pointed n-unipotent objects $(\mathcal{V},v)$ there exists a morphism of pointed n-unipotent objects*

$$(\mathcal{E},e) \longrightarrow (\mathcal{V},v).$$

Finally, a universal pointed pro-object in $\mathcal{C}$ is a compatible sequence $\{(\mathcal{E}_n,e_n)\}_{n\geq 1}$ of universal pointed n-unipotent objects in $\mathcal{C}$, equipped with maps of pointed objects

$$(\mathcal{E}_n,e_n) \longrightarrow (\mathcal{E}_{n-1},e_{n-1}).$$

Note that if a universal pointed n-unipotent object exists, it is unique up to unique isomorphism. Since we have a canonical identification of $\omega(\mathcal{A}_n(\mathcal{C},\omega))$ with $A_n(\mathcal{C},\omega)$, we have an associated n-unipotent pointed object $(\mathcal{A}_n(\mathcal{C},\omega),1)$. Furthermore, the quotient map $A_{n+1}(\mathcal{C},\omega) \to A_n(\mathcal{C},\omega)$ induces transition maps

$$(\mathcal{A}_{n+1}(\mathcal{C},\omega),1) \longrightarrow (\mathcal{A}_n(\mathcal{C},\omega),1)\,.$$

From the equivalence between representation of $\pi_1(\mathcal{C},\omega)$ and left $A(\mathcal{C},\omega)$-modules, we obtain:

Lemma A.3. *The inverse system $\{(\mathcal{A}_n(\mathcal{C},\omega),1)\}_{n\geq 1}$ is a universal pointed pro-object in $\mathcal{C}$.*

A.1.2. *Path torsors.* As in the topological case, we can define path torsors of the universal objects $\mathcal{A}_n(\mathcal{C},\omega)$ in unipotent neutral Tannakian categories. If ν is another fibre functor of $\mathcal{C}$, then recall there are corresponding path torsors

$$\pi_1(\mathcal{C};\omega,\nu)$$

for the Tannakian fundamental group, given by the tensor compatible isomorphisms between ω and ν. We define likewise

$$A_n(\mathcal{C};\omega,\nu) := A_n(\mathcal{C},\omega) \times_{\pi_1(\mathcal{C},\omega)} \pi_1(\mathcal{C};\omega,\nu)$$

where the product is interpreted in the following sense: The co-ordinate ring $\mathcal{O}(\pi_1(\mathcal{C};\omega,\nu))$ has the structure of a free $\mathcal{O}(\pi_1(\mathcal{C},\omega))$-comodule of rank one, giving $\mathcal{O}(\pi_1(\mathcal{C};\omega,\nu))^*$ the structure of a free $\mathcal{O}(\pi_1(\mathcal{C},\omega))^*$-module of rank 1 hence we may define

$$A_n(\mathcal{C};\omega,\nu) := \left((\mathcal{O}(\pi_1(\mathcal{C};\omega,\nu))^* \otimes_{\mathcal{O}(\pi_1(\mathcal{C};\omega))^*} A_n(\mathcal{C},\omega)^*\right)^*.$$

In the topological setting, the universal pointed cover has the following useful property. For any point $x \in X$, there is a canonical isomorphism

$$\pi_1(X;b,x) \simeq p^{-1}(x).$$

In the case of a neutral unipotent Tannakian category we have the following analogue, see for instance Kim [Kim09, §1] or Betts [Bet17, §6.2.2].

Lemma A.4. *Let ω and ν be fibre functors, and let ω_n and ν_n denote their restriction to the full subcategory of n-unipotent objects. Then we have functorial isomorphisms*

$$\nu(\mathcal{A}_n(\mathcal{C},\omega)) \simeq A_n(\mathcal{C};\omega,\nu) \simeq \omega(\mathcal{A}_n(\mathcal{C},\nu)).$$

Proof. By the universal property of $\mathcal{A}_n$, the map

$$\begin{aligned} \mathrm{Hom}(\omega_n, \nu_n) &\longrightarrow \nu(\mathcal{A}_n(\mathcal{C}, \omega)) \\ F &\longmapsto F(\mathcal{A}_n)(e_n) \end{aligned}$$

is an isomorphism of K-vector spaces. Since $\mathrm{Hom}(\omega_n, \omega_n) = A_n(\mathcal{C}, \omega)$ we get a map

$$\pi_1(\mathcal{C}; \omega, \nu) \times_{\pi_1(\mathcal{C},\omega)} A_n(\mathcal{C}, \omega) \longrightarrow \mathrm{Hom}(\omega_n, \nu_n) \ : \ (\gamma, x) \longmapsto \gamma \circ x.$$

Since both sides are free $A_n(\mathcal{C}, \omega)$-modules of rank one, this is an isomorphism.

For the second isomorphism, note that by duality we have an isomorphism $\mathrm{Hom}(\omega_n, \nu_n) \simeq \mathrm{Hom}(\nu_n, \omega_n)$, (i.e. the isomorphism is defined by sending $f \in \mathrm{Hom}(\omega_n, \nu_n)$ to the morphism of functors f^* sending $V \in \mathcal{C}$ to $f^*(V) := (f(V))^*$). □

The identification of $A_n(\mathcal{C}; \omega, \nu)$ with $\mathrm{Hom}(\omega_n, \nu_n)$ induces composition maps

$$A_n(\mathcal{C}; \omega_2, \omega_3) \times A_n(\mathcal{C}; \omega_1, \omega_2) \to A_n(\mathcal{C}; \omega_1, \omega_3)$$

for all fibre functors $\omega_1, \omega_2, \omega_3$. We may also describe the right action of $A_n(\mathcal{C}, \omega)$ on $\nu(\mathcal{A}_n(\mathcal{C}, \omega))$ induced by these isomorphisms. Given $x \in \nu(\mathcal{A}_n(\mathcal{C}, \omega))$, and $y \in A_n(\mathcal{C}; \omega, \nu)$, the product $y.x$ is defined as follows. Take $\widetilde{x}$ to be the unique endomorphism $\mathcal{A}_n(\omega)$ such that $\nu\widetilde{x}(e_n) = x$. Then

$$y.x = \widetilde{x}(y).$$

A.2. **Unipotent isocrystals on $\mathcal{X}_{\mathbf{F}_p}$.** We now recall some foundational results about the category of unipotent isocrystals on a curve over $\mathbf{F}_p$ [Ber96, CS99]. We first recall the notion of a rigid triple, and then define the category $\mathcal{C}^{\mathrm{rig}}(\mathcal{X}_{\mathbf{F}_p})$.

We start by recalling the notion of a rigid triple. Related notions are those of a *triple* in [CT03], or a $\mathbf{Q}_p$-*frame* in [LS07]. A *rigid triple* over $\mathbf{F}_p$ is a triple (Y, X, P), where

- P is a formal p-adic $\mathbf{Z}_p$ scheme,
- X is a closed $\mathbf{F}_p$-subscheme of P, proper over $\mathbf{F}_p$,
- $Y \subset X$ is an open $\mathbf{F}_p$-subscheme such that P is smooth in a neighbourhood of Y.

Given a rigid triple (Y, X, P), we let $P_{\mathbf{Q}_p}$ denote the Raynaud generic fibre of P. We let

$$]Y[\subset P_{\mathbf{Q}_p}$$

denote the tube of Y, which consists of all the points that reduce to a point of Y. Finally, let $j^\dagger\mathcal{O}_Y$ be the overconvergent structure sheaf on $]Y[$, as defined in [Ber96, §2.1.1.3].

Definition A.5. *Let $T = (Y, X, P)$ be a rigid triple. An overconvergent isocrystal on T is a locally free $j^\dagger\mathcal{O}_Y$-module with connection.*

Given rigid triples $T = (Y, X, P)$ and $T' = (Y', X', P')$, and a morphism $f : Y \to Y'$, a *compatible morphism* $T \to T'$ is a morphism

$$g : \mathcal{W} \longrightarrow P'_{\mathbf{Q}_p}$$

from a strict neighbourhood of $]Y[$ to $P'_{\mathbf{Q}_p}$, which is compatible with f via the specialisation map.

Given two rigid triples $T = (Y, X, P)$ and $T' = (Y, X, P')$, there is a canonical equivalence between the category of overconvergent isocrystals on T and T', via the category of overconvergent isocrystals on $(Y, X, P \times_{\mathbf{Z}_p} P')$, (see [Ber96, §2.3.1] or [LS07, §7.3.11]). For this reason we often suppress the choice of rigid triple from our notation and terminology, and denote the category of unipotent isocrystals on Y by $\mathcal{C}^{\mathrm{rig}}(Y)$. The category $\mathcal{C}^{\mathrm{rig}}(T)$ is sometimes referred to as a *realisation* of $\mathcal{C}^{\mathrm{rig}}(Y)$. By functoriality, for any $y \in Y(\mathbf{F}_p)$, we obtain a functor y^* from $\mathcal{C}^{\mathrm{rig}}(Y)$ to the category $\mathcal{C}^{\mathrm{rig}}(\mathrm{Spec}\,\mathbf{F}_p)$ of unipotent

isocrystals on $\operatorname{Spec}\mathbf{F}_p$, which is canonically identified with the category of $\mathbf{Q}_p$-vector spaces, via the realisation given by the rigid triple

$$T = (\operatorname{Spec}\mathbf{F}_p, \operatorname{Spec}\mathbf{F}_p, \operatorname{Spf}\mathbf{Z}_p).$$

In this way y^* can be viewed as a fibre functor on the unipotent Tannakian category $\mathcal{C}^{\mathrm{rig}}(Y_{\mathbf{F}_p})$.

An explicit description of the fibre functor y^* may be given as follows. Choose a lift $\widetilde{y}$ of y to $]Y[$. Then $\widetilde{y}$ defines a fibre functor on $\mathcal{C}^{\mathrm{rig}}(T)$ in the obvious way. Whenever we write the fibre functor y^* in this paper we shall mean $\widetilde{y}^*$ for some choice of $\widetilde{y}$. The justification for this notation is that if $\widetilde{y}_1$ and $\widetilde{y}_2$ are two different lifts, then there is an isomorphism of functors

$$T_{\widetilde{y}_1,\widetilde{y}_2} : \widetilde{y}_1 \to \widetilde{y}_2$$

defined by parallel transport as follows. Given an overconvergent isocrystal $(\mathcal{V},\nabla)$ on T, the pullback of $(\mathcal{V},\nabla)$ to $]y[$, and hence the maps

$$\mathcal{V}(]y[)^{\nabla=0} \xrightarrow{\simeq} \widetilde{y}_i^*\mathcal{V}$$

are bijective. The natural transformation $T_{\widetilde{y}_1,\widetilde{y}_2}(\mathcal{V},\nabla)$ is defined as the composite

$$\widetilde{y}_1^*\mathcal{V} \xleftarrow{\simeq} \mathcal{V}(]y[)^{\nabla=0} \xrightarrow{\simeq} \widetilde{y}_2^*\mathcal{V}.$$

The main example of interest to us is the following. Using the notation of § 4.1, we denote $\mathcal{C}^{\mathrm{rig}}(\mathcal{X}_{\mathbf{F}_p})$ for the Tannakian category of unipotent isocrystals on the rigid triple

$$T = (\mathcal{X}_{\mathbf{F}_p}, \mathcal{X}_{\mathbf{F}_p}, \mathfrak{X}),$$

where $\mathfrak{X}$ is the completion of $\mathcal{X}$ along its special fibre. This will usually be referred to simply as the category of unipotent isocrystals on $\mathcal{X}_{\mathbf{F}_p}$. Its fundamental group will be denoted by

$$\pi_1^{\mathrm{rig}}(\mathcal{X}_{\mathbf{F}_p}, \bar{b}) := \pi_1(\mathcal{C}^{\mathrm{rig}}(\mathcal{X}_{\mathbf{F}_p}); \bar{b})$$

and the maximal n-unipotent quotient and its path torsors are denoted $\mathrm{U}_n^{\mathrm{rig}}(\bar{b})$ and $\mathrm{U}_n^{\mathrm{rig}}(\bar{b},\overline{x})$. We also use the notation:

$$\begin{cases} A_n^{\mathrm{rig}}(\bar{b}) & := & A_n(\mathcal{C}^{\mathrm{rig}}(\mathcal{X}_{\mathbf{F}_p}); \bar{b}^*), \\ A_n^{\mathrm{rig}}(\bar{b},\overline{x}) & := & A_n(\mathcal{C}^{\mathrm{rig}}(\mathcal{X}_{\mathbf{F}_p}); \bar{b}^*, \overline{x}^*). \end{cases}$$

as well as the notation $\mathcal{A}_n^{\mathrm{rig}}(\bar{b})$ for the corresponding universal n-unipotent object. When we want to emphasise the choice of a rigid triple (Y,X,P), we write $A_n^{\mathrm{rig}}(b,x)$ and $A_n^{\mathrm{rig}}(b)$, where b,x are $\mathbf{Q}_p$ points of $P_{\mathbf{Q}_p}$ lying above $\bar{b}$ and $\overline{x}$ respectively.

References

[AS05] Amod Agashe and William Stein. Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero. *Math. Comp.*, 74(249):455–484, 2005. With an appendix by J. Cremona and B. Mazur. ↑6.2.

[Bar14a] B. Baran. An exceptional isomorphism between modular curves of level 13. *J. Number Theory*, 145:273–300, 2014. ↑1.1, 1.1, 6.3.

[Bar14b] B. Baran. An exceptional isomorphism between modular curves of level 13 via Torelli's theorem. *Math. Res. Lett.*, 21(5):919–936, 2014. ↑1.1, 1.1, 6.2.

[BB15] Jennifer S. Balakrishnan and Amnon Besser. Coleman-Gross height pairings and the p-adic sigma function. *J. Reine Angew. Math.*, 698:89–104, 2015. ↑1.5.

[BBM16] Jennifer S. Balakrishnan, Amnon Besser, and J. Steffen Müller. Quadratic Chabauty: p-adic heights and integral points on hyperelliptic curves. *J. Reine Angew. Math.*, 720:51–79, 2016. ↑1.5.

[BBM17] Jennifer S. Balakrishnan, Amnon Besser, and J. Steffen Müller. Computing integral points on hyperelliptic curves using quadratic Chabauty. *Math. Comp.*, 86:1403–1434, 2017. ↑1.5.

[BCP97] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *J. Symb. Comp*, 24(3-4):235–265, 1997. ↑1.7, 6.1.

[BD16] Jennifer S. Balakrishnan and Netan Dogra. Quadratic Chabauty and rational points I: p-adic heights. *To appear in Duke Math. J., arXiv:1601.00388*, 2016. ↑1.5, 1.6, 1.7, 2, 2.1, 2.2, 2.3, 3, 3.4, 3.6.

[BD17] Jennifer S Balakrishnan and Netan Dogra. Quadratic Chabauty and rational points II: Generalised height functions on Selmer varieties. *arXiv preprint arXiv:1705.00401*, 2017. ↑1.6, 1.7, 2.3, 3.6, 3.8, 4, 4.2, 4.3, 4.5, 5.

[BDCKW] Jennifer S. Balakrishnan, Ishai Dan-Cohen, Minhyong Kim, and Stefan Wewers. A non-abelian conjecture of Tate-Shafarevich type for hyperbolic curves. *Mathematische Annalen*. To appear. ↑1.3.

[BDM$^+$] J.S. Balakrishnan, N. Dogra, J.S. Müller, J. Tuitman, and J. Vonk. Magma code. https://github.com/jtuitman/Cartan13. ↑1.7, 6.4.1, 6.5.

[Ber96] P. Berthelot. Cohomologie rigide et cohomologie rigide a supports propres. *Preprint*, 1996. ↑A.2, A.2.

[Bet17] L Alexander Betts. The motivic anabelian geometry of local heights on abelian varieties. *arXiv preprint arXiv:1706.04850*, 2017. ↑A.1.2.

[BK90] Spencer Bloch and Kazuya Kato. L-functions and Tamagawa numbers of motives. In *The Grothendieck Festschrift, Vol. I*, volume 86 of *Progr. Math.*, pages 333–400. Birkhäuser Boston, Boston, MA, 1990. ↑2.1, 2.1.

[BL04] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2004. ↑2.4.

[BO83] P. Berthelot and A. Ogus. F-isocrystals and de Rham cohomology I. *Invent. Math.*, 72:159–199, 1983. ↑4.5.

[BP11] Y. Bilu and P. Parent. Serre's uniformity problem in the split Cartan case. *Ann. of Math. (2)*, 173(1):569–584, 2011. ↑1.1.

[BPR13] Y. Bilu, P. Parent, and M. Rebolledo. Rational points on $X_0^+(p^r)$. *Ann. Inst. Fourier*, 63(3):957–984, 2013. ↑1.1.

[BPS16] Nils Bruin, Bjorn Poonen, and Michael Stoll. Generalized explicit descent and its application to curves of genus 3. *Forum Math. Sigma*, 4:e6, 80, 2016. ↑6.3.

[Bru03] N. Bruin. Chabauty methods using elliptic curves. *J. Reine. Angew. Math*, 562:27–49, 2003. ↑2.

[BS09] Nils Bruin and Michael Stoll. Two-cover descent on hyperelliptic curves. *Math. Comp.*, 78:2346–2370, 2009. ↑2.

[BT17] Jennifer S. Balakrishnan and Jan Tuitman. Explicit Coleman integration for curves. *Arxiv preprint*, 2017. ↑6.6.

[CG89] Robert F. Coleman and Benedict H. Gross. p-adic heights on curves. In *Algebraic number theory*, volume 17 of *Adv. Stud. Pure Math.*, pages 73–81. Academic Press, Boston, MA, 1989. ↑1.5.

[Cha41] C. Chabauty. Sur les points rationels des courbes algébriques de genre supérieur à l'unité. *C.R. Acad. Sci.*, 212:882–884, 1941. ↑1.3.

[Che98] Imin Chen. The jacobians of non-split cartan modular curves. *Proceedings of the London mathematical society*, 77(1):1–38, 1998. ↑1.1.

[CK10] J. Coates and M. Kim. Selmer varieties for curves with CM Jacobians. *Kyoto J. Math.*, 50(4):827–852, 2010. ↑2.2, 2.3, 3.4.

[Col85] Robert F. Coleman. Effective Chabauty. *Duke Mathematical Journal*, 52(3):765–770, 1985. ↑1.3.

[CS99] B. Chiarellotto and B. Le Stum. F-isocristaux unipotents. *Compositio Math.*, 116:81–110, 1999. ↑5.1, 5.2, A.2.

[CT03] Bruno Chiarellotto and Nobuo Tsuzuki. Cohomological descent of rigid cohomology for étale coverings. *Rendiconti del Seminario Matematico della Università di Padova*, 109:63–215, 2003. ↑A.2.

[DC17] Ishai Dan-Cohen. Mixed Tate motives and the unit equation II. *Arxiv preprint*, 2017. ↑1.3.

[DCW15] Ishai Dan-Cohen and Stefan Wewers. Explicit Chabauty-Kim theory for the thrice punctured line in depth 2. *Proc. Lond. Math. Soc. (3)*, 110(1):133–171, 2015. ↑1.3.

[DCW16] Ishai Dan-Cohen and Stefan Wewers. Mixed Tate motives and the unit equation. *Int. Math. Res. Not. IMRN*, (17):5291–5354, 2016. ↑1.3.

[DDLR15] Henri Darmon, Michael Daub, Sam Lichtenstein, and Victor Rotger. Algorithms for Chow-Heegner points via iterated integrals. *Mathematics of Computation*, 84(295):2505–2547, 2015. ↑3.10.

[Del89] P. Deligne. Le groupe fondamental de la droite projective moins trois points. In *Galois groups over* $\mathbf{Q}$, volume 16 of *Math. Inst. Res. Inst. Publ.*, pages 79–297. Springer-Verlag, 1989. ↑2.1.

[Del90] P. Deligne. Catégories tannakiennes. In *The Grothendieck Festschrift, Vol. II*, volume 87 of *Progr. Math.*, pages 111–195. Birkhäuser Boston, Boston, MA, 1990. ↑A.1.1.

[DRS12] H. Darmon, V. Rotger, and I. Sols. Iterated integrals, diagonal cycles, and rational points on elliptic curves. *Publ. Math. de Besançon*, 2:19–46, 2012. ↑3.10.

[Edi89] B. Edixhoven. *Stable models of modular curves and applications*. PhD thesis, Utrecht, 1989. ↑6.2, 6.4, 6.2, 6.6.

[Edi90] B. Edixhoven. Minimal resolution and stable reduction of $X_0(N)$. *Ann. Inst. Fourier*, 40(1):31–67, 1990. ↑6.2, 6.2.

[EH17] Jordan S. Ellenberg and Daniel Rayor Hast. Rational points on solvable curves over $\mathbb{Q}$ via non-abelian chabauty. *ArXiv preprint*, 2017. ↑2.2, 2.3.

[FW99] E.V. Flynn and J.L. Wetherell. Finding rational points on bielliptic genus 2 curves. *Manuscripta Math.*, 100(4):519–533, 1999. ↑2.

[Gal02] Steven D. Galbraith. Rational points on $X_0^+(N)$ and quadratic $\mathbb{Q}$-curves. *J. Théor. Nombres Bordeaux*, 14(1):205–219, 2002. ↑1.1.

[GZ86] B. Gross and D. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986. ↑6.2.

[Had11] M. Hadian. Motivic fundamental groups and integral points. *Duke Math. J.*, 160(3):503–565, 2011. ↑1.6, 4.3.

[Kim05] Minhyong Kim. The motivic fundamental group of $\mathbf{P}^1 - \{0, 1, \infty\}$ and the theorem of Siegel. *Inventiones mathematicae*, 161(3):629–656, 2005. ↑1.3, 2.1.

[Kim09] M. Kim. The unipotent Albanese map and Selmer varieties for curves. *Publ. RIMS*, 45:89–133, 2009. ↑1.3, 1.6, 2, 2.1, 2.1, 2.1, 2.2, 2.2, 4.2, 4.2, A.1.2.

[KL89] V. A. Kolyvagin and D. Yu. Logachëv. Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties. *Algebra i Analiz*, 1(5):171–196, 1989. ↑6.2.

[KM85] N. Katz and B. Mazur. *Arithmetic moduli of elliptic curves*, volume 108 of *Annals of Math. Studies*. Princeton University Press, 1985. ↑6.4.

[KT08] M. Kim and A. Tamagawa. The l-component of the unipotent Albanese map. *Math. Ann.*, 340(1):223–235, 2008. ↑3.4.

[LS07] Bernard Le Stum. *Rigid cohomology*, volume 172. C.U.P., 2007. ↑A.2, A.2.

[Maz77] B. Mazur. Modular curves and the Eisenstein ideal. *IHÉS Publ. Math.*, 47:33–186, 1977. ↑2.3.

[Maz78] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978. ↑1.1.

[Mer96] Loïc Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3):437–449, 1996. ↑2.3.

[Mum70] D. Mumford. *Abelian varieties*. Number 5 in Tata Institute of Fundamental Research Studies in Mathematics. Tata Institute of Fundamental Research, Bombay, 2nd edition edition, 1970. ↑2.4.

[Nek93] J. Nekovar. On p-adic height pairings. In *Séminaire de Théorie des Nombres, Paris 1990-1991*, pages 127–202. Birkhäuser, 1993. ↑1.5, 3, 3.1, 3.1, 3.1, 3.2, 3.3, 3.3.

[Ols11] M. Olsson. Towards non-abelian p-adic Hodge theory in the good reduction case. *Memoirs of the AMS*, (990), 2011. ↑2.1, 5.3.

[Ray90] M. Raynaud. p-Groupes et réduction semi-stable des courbes. In P. Cartier, editor, *The Grothendieck Festschrift, vol. III*, volume 88 of *Progr. Math.*, pages 179–197. Birkhäuser, 1990. ↑6.6.

[Ray94] M. Raynaud. 1-motifs et Monodromie Géométrique. *Astérisque*, 223:295–319, 1994. Périodes p-adiques (Bures-sur-Yvette, 1988). ↑3.2.

[Rib80] K. Ribet. Twists of modular forms and endomorphisms of abelian varieties. *Math. Ann.*, 253:43–62, 1980. ↑6.1.

[Sch12] R. Schoof. The Mordell-Weil group of a modular curve of level 13. *Unpublished manuscript*, 2012. ↑6.3.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972. ↑1.1.

[Ser97] Jean-Pierre Serre. *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, third edition, 1997. ↑1.4.

[Ser02] Jean-Pierre Serre. *Galois cohomology*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2002. ↑3.4.

[Shi70] G. Shimura. On canonical models of arithmetic quotients of bounded symmetric domains. *Ann. of Math.*, 91:144–222, 1970. ↑6.1.

[Sik17] Samir Siksek. Quadratic Chabauty for modular curves. *Arxiv preprint*, 2017. ↑1.5.

[Tui16] Jan Tuitman. Counting points on curves using a map to $\mathbf{P}^1$. *Mathematics of Computation*, 85(298):961–981, 2016. ↑1.7, 5.4, 6.3, 6.4, 6.5.

[Tui17] Jan Tuitman. Counting points on curves using a map to $\mathbf{P}^1$, II. *Finite Fields Appl.*, 45:301–322, 2017. ↑1.7, 5.4, 6.3, 6.4.

Jennifer S. Balakrishnan, Department of Mathematics and Statistics, Boston University, 111 Cummington Mall, Boston, MA 02215, USA

E-mail address: jbala@bu.edu

Netan Dogra, Department of Mathematics, Imperial College London, London SW7 2AZ, UK

E-mail address: n.dogra@imperial.ac.uk

J. Steffen Müller, Bernoulli Institute, University of Groningen, Nijenborgh 9, 9747 AG Groningen, The Netherlands

E-mail address: steffen.muller@rug.nl

Jan Tuitman, KU Leuven, Departement Wiskunde, Celestijnenlaan 200B, 3001 Leuven, Belgium

E-mail address: jan.tuitman@kuleuven.be

Jan Vonk, Department of Mathematics and Statistics, McGill University, Montréal H3A 0B9, Canada

E-mail address: jan.vonk@math.mcgill.com